CORINEX User Guide

Low Voltage and High Density Compact Gateway

for last mile solution

November 28, 2012

CORPORATE HEADQUARTERS
CORINEX COMMUNICATIONS
1200 - 570 Granville Street
Vancouver BC V6C 3P1, Canada
Tel: +1 604 692 0520
Fax: +1 604 964 0061
URL: www.corinex.com

COPYRIGHT

This document, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of the license. The content of this document is furnished for informational use only, it is subject to change without notice and it does not represent a commitment on the part of Corinex Communications Corp.

Corinex Communications Corp. assumes no responsibility or liability for any errors or inaccuracies that may appear in this document. It is our policy to enhance our products as new technologies, hardware components, software and firmware become available; therefore, the information contained in this document is subject to change without notice.

Some features, functions, and operations described in this document may not be included and sold in certain countries due to government regulations or marketing policies.

The use of the product or its features described in this document may be restricted or regulated by law in some countries. If you are unsure which restrictions or regulations apply, you should consult your regional Corinex office or the authorized reseller.

Published by:

Corinex Communications Corp.

1200 – 570 Granville Street

Vancouver, B.C. Canada V6C 3P1

Tel.:+1 604 692 0520

Fax: +1 604 694 0061

ww.corinex.com

Corinex is a registered trademark of Corinex Communications Corp. Microsoft, MS-DOS, MS; Windows are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries. All products or company names mentioned herein may be the trademarks of their respective owners.

Copyright (c) 2001-2011 by Corinex Communications Corp.

NOTE: This equipment has been tested and found to comply with the limits for Class B information technology equipment. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference, the end user is advised to take adequate measures.

Revision History:

V1.5 – November 28, 2012 – Added safety, maintenance, packaging section

V1.4 – November 16, 2012 – Correction on the number of PLC ports of HD compact gateways

V1.3 – October 4, 2012 – Updated LED functions description and gateway pictures

V1.2 – October 3, 2011 – Changed IND to LV

V1.1 – September 21, 2011 – Added AC connector pin info

V1.0 – September 13, 2011

END USER LICENSE AGREEMENT

This End User License Agreement (EULA) is a legal agreement between you and CORINEX COMMUNICATIONS CORPORATION (CORINEX) with regard to the copyrighted Software provided with this EULA.

Use of any software and related documentation (Software) provided with CORINEX hardware product, or made available to you by CORINEX via download or otherwise, in whatever form or media, will constitute your acceptance of these terms, unless separate terms are provided by the software supplier, in which case certain additional or different terms may apply. If you do not agree with the terms of this EULA, do not download, install, copy or use the Software.

1 License Grant. CORINEX grants to you a personal, non-transferable and non-exclusive right to use the copy of the Software provided with this EULA. You agree you will not copy the Software except as necessary to use it on a single hardware product system. You agree that you may not copy the written materials accompanying the Software. Modifying, translating, renting, copying, transferring or assigning all or part of the Software, or any rights granted hereunder, to any other persons, and removing any proprietary notices, labels or marks from the Software is strictly prohibited. Furthermore, you hereby agree not to create derivative works based on the Software. You may permanently transfer all of your rights under this EULA, provided you retain no copies, you transfer all of the Software, and the recipient agrees to the terms of this EULA. If the Software is an upgrade, any transfer must include all prior versions of the Software.

2 Copyright. The Software is licensed, not sold. You acknowledge that no title to the intellectual property in the Software is transferred to you. You further acknowledge that title and full ownership rights to the Software will remain the exclusive property of Corinex Communications Corporation and/or its suppliers, and you will not acquire any rights to the Software, except as expressly set forth above. All copies of the Software will contain the same proprietary notices as contained in or on the Software.

3 Reverse Engineering. You agree that you will not attempt, and if you are a corporation, you will use your best efforts to prevent your employees and contractors from attempting to reverse compile, modify, translate or disassemble the Software in whole or in part. Any failure to comply with the above or any other terms and conditions contained herein will result in the automatic termination of this license and the reversion of the rights granted hereunder to CORINEX.

4 Disclaimer of Warranty. The Software is provided “AS IS “without warranty of any kind. CORINEX and its suppliers disclaim and make no express or implied warranties and specifically disclaim warranties of merchantability, fitness for a particular purpose and non-infringement of third-party rights. The entire risk as to the quality and performance of the Software is with you. Neither CORINEX nor its supplier’s warrant that the functions contained in the Software will meet your requirements or that the operation of the Software will be uninterrupted or error-free.

5 Limitation of Liability. Corinex’s entire liability and your exclusive remedy under this EULA shall not exceed the price paid for the Software, if any. In no event shall CORINEX or its suppliers be liable to you for any consequential, special, incidental or indirect damages of any kind arising out of the use or inability to use the software, even if CORINEX or its supplier has been advised of the possibility of such damages, or any claim by a third party.

6 Applicable Laws. This EULA will be governed by the laws of Canada, excluding its conflict of law provisions.

7 Export Laws. This EULA involves products and/or technical data that may be controlled under any applicable export control laws, and regulation, and may be subject to any approval required under such laws and regulations.

8 Precedence. Except as set out above, where separate terms are provided by the software supplier, then, subject to this EULA, those terms also apply and prevail, to the extent of any inconsistency with this EULA.

IMPORTANT SAFETY INSTRUCTIONS

We have provided important safety messages in this manual and on your device. Always read and obey all safety messages.

- **DO NOT** open the cover of the device when it is connected to a power source AC or DC.
- **DO NOT** use if the AC or DC power cord is damaged.
- **Do NOT** submerge the device into water.
- **DO NOT** immerse cord or plug in water.
- **STOP** using the device immediately if it emits excessive noise.
- **DO NOT** store flammable materials next to, on top of the device.
- Keep cord away from heated surfaces.
- Check for any damage on the connectors before use.
- The device is protected against low pressure water jets from any direction. Limited ingress permitted.
- The device is completely protected against dust ingress.

Table of Contents

INTRODUCTION **8**

FEATURES AND TECHNICAL DATA **9**

LV AND HD COMPACT GATEWAY PRODUCT OPTIONS **10**

Low Voltage Compact Gateway (CXP - LVC - GWYC) 10

High Density Compact Gateway (CXP - HDC - GWYC) 10

Integrated Couplers 10

INSTALLATION AND REQUIREMENTS **11**

CONNECTING AND POWERING THE LV AND HD COMPACT GATEWAY **12**

CONNECTING THE AC WIRE **13**

BUTTON AND LEDS **14**

Buttons 14

LEDS 15

DEFAULT CONFIGURATION SETTINGS **16**

FIRMWARE AND DEVICE STRUCTURE **17**

Web Interface 19

CONFIGURATIONS AND SETTINGS **20**

Preparing DHCP/TFTP server 20

Step 1: Turning off Windows Firewall from the Control Panel 20

Step 2: Installing DHCP server 20

Step 3: Preparing the network interface on the PC 20

Step 4: Setting a default interface for DHCP server 21

Step 5: Setting a standard profile for DHCP server 22

Preparing Telnet PuTTY for command line interface (CLI) console 23

Loading auto - configuration file (*.conf) 24

Step 1: Preparing an auto - configuration file 24

Step 2: Preparing a DHCP profile to download auto - configuration 25

Step 3: Binding a DHCP profile with static IP table 26

Step 4: Rebooting the modem and checking the loading process 27

Step 5: Loading auto - configuration files to other modems 28

EXAMPLE OF DEPLOYMENT **29**

TECHNICAL SPECIFICATIONS **32**

MAINTENANCE **33**

PROCEDURES OF PACKAGING, TRANSPORT AND STORAGE 34

ANNEX 1: CORINEX AV200 ENTERPRISE FEATURES 37

Introduction 37

Application Description 37

Core Features 37

MAC Layer 42

Application Layer 44

PLC Application Description 49

Boot Process 54

Constraints for Network Design 56

ANNEX 2: EXAMPLE OF CONFIGURATION FILES 58

Master Access Mode 6 (HE/LV 6) output to coaxial port 58

Master Access Mode 1 (HE/LV 1) output to pin 3 and 4 58

Master Access Mode 2 (HE/LV 2) output to pin 3 and 4 58

Master Access Mode 3 (HE/LV 3) output to pin 3 and 4 59

Slave End User (CPE/EU) output to pin 3 and 4 59

TD Repeater (TDR/LV) output to pin 3 and 4 59

Master Access Mode 6 (HE/LV 6) with VLAN and OVLAN parameters 60

Slave End User (CPE/EU) with VLAN 101 and OVLAN parameters 61

Slave End User (CPE/EU) with VLAN 102 and OVLAN parameters 62

INTRODUCTION

This user guide describes the basic features and specifications of the LV and HD Compact Gateways, as well as the basic configuration and installation options. Two additional manuals are available on the documentation CD and the Corinex webpage. The *Alma Auto-configuration Manual* details the auto-configuration process and options, and the *SNMP Manual* explains the MIB architecture.

The Low Voltage Compact Gateway (LV) and the High Density Compact Gateway (HD) are Corinex's BPL access product line using 200-Mbps AV200 Technology. The Gateways allow an easy installation to Multi Dwelling Units (MDUs) or last mile access neighborhoods where the Gateway acts as a head-end modem, extending an internet connection (optical fiber, DSL, or wireless access) either to a power line or coaxial cable infrastructure, depending on the customer's requirements. The modem allows users to extend an internet connection to a power line or cable network within an MDU, without the need for installing new wiring. End users can connect their Ethernet enabled devices such as PC, VoIP phones, Media Centers, etc., using the Corinex AV200 series of Powerline or CableLAN Ethernet Adapters, to any electrical or coaxial socket in their premise to access the Internet.

The LV and HD Compact Gateways can serve large networks, up to 1,024 network devices. And by embedding three-phase coupler inside the rugged enclosures, the Gateways provide easy installation for three-phase power system deployment. AV200 Powerline technology by Corinex also provides numerous networking possibilities with physical layer transfer rates of up to 200 Mbps depending on the characteristics of the power line media. OFDM technology and the powerful error correction system used in AV200 technology allow for robust performance under harsh conditions in electrical or coaxial networks. The LV and HD Compact Gateways also support other external couplers that can be used to inject the BPL signal by connecting through the coaxial cable port.

FEATURES AND TECHNICAL DATA

Corinex Low Voltage Compact Gateway and High Density Compact Gateways are high performance BPL modem devices designed for low-voltage power line access networks in either single phase three-wire or three-phase four-wire systems. The Gateway is ideal for use as a Head-End unit to control a last mile low-voltage access network as well as a large In-Building distribution network. Used with Time Division Repeater units, it can extend the coverage of a PLC network beyond 100 users.

LV and HD Compact Gateways always come with basic features that include:

- Special housing for installations in rough environments like transformer stations and street cabinets
- Ability to configure as a Head-End Master (HE), Time Division Repeater (TDR), or Slave (CPE) unit - same as other AV200 Enterprise products by loading auto-configuration settings
- Physical throughput connectivity of up to 200 Mbps
- 802.1Q VLAN & Optimized VLANs (OVLAN)
- 128-bit AES, 256-bit AES, and 3DES hardware encryption
- Integrated 802.1D Ethernet Bridge with Rapid or Common Spanning Tree Protocol
- Quality of Service (QoS) and 8-level priority queues, with programmable priority-classification Engine
- Priority classification according to 802.1P tags, IP coding (IPv4 or Ipv6) or TCP source/destination ports
- 10/100BaseT Fast Ethernet interface for connection to the network point of presence
- CSMA/CARP (Carrier Sense Multiple Access with Collision Avoidance and Resolution using priorities protocol)
- Bridge Forwarding Table for 128 MAC addresses (LV) or 1,024 MAC addresses (HD)
- Optimized support for broadcast and multicast traffic
- SNMP agent to facilitate management of larger networks
- Integrated three phase coupler

LV AND HD COMPACT GATEWAY PRODUCT OPTIONS

Corinex LV and HD Compact Gateways come with a variation of models that users can choose to match with their requirement and deployment type.

Low Voltage Compact Gateway (CXP-LVC-GWYC)

The LV Compact Gateway can run as an HE master modem to serve a BPL network of up to 128 MAC addresses. It can connect to maximum 31 TDR or CPE modems directly. This basic modem can be used in a small-size network. The following interfaces and connectors are provided on the Gateway:

- RJ-45 Ethernet Interface for accessing Ethernet network,
- RS485 Serial Port,
- Female TNC-type connector for providing BPL access on a coaxial cable,
- 4-pin power socket for power and providing BPL access on the power line,
- 4-pin socket for DC backup power supply.

High Density Compact Gateway (CXP-HDC-GWYC)

The High Density Compact Access Gateway can serve as a Head-End Master modem in a BPL network comprising of network devices with up to 1,024 MAC addresses in total. HD Gateway has a capacity to provide direct connection to maximum 15 TDR or CPE modems. Each of the TDR modems can extend the distance reach and a number of connecting CPE modems. It is recommended to use the HD Gateway in a medium or large-size network. The following interfaces and connectors are provided on the Gateway:

- RJ-45 Ethernet Interface for accessing Ethernet network,
- RS485 Serial Port,
- Female TNC-type connector for providing BPL access on a coaxial cable,
- 4-pin power socket for power and providing BPL access on the power line,
- 4-pin socket for DC backup power supply.

Integrated Couplers

Both the LV and HD Compact Gateways are integrated with internal three-phase coupler which provides easy installation on the three-phase power line system. The integrated coupler connection is a 4-pin socket for coupling the signal to line and neutral wires of the three-phase four-wire power line. With this feature, Corinex LV and HD Compact Gateways are capable to provide a last mile solution anywhere worldwide. Integration of the internal coupler eliminates a need for external coupler and minimizes the insertion and connector losses caused by an external coupler.

INSTALLATION AND REQUIREMENTS

The LV and HD Compact Gateways by Corinex are network devices mainly used for last mile solutions in broadband access technology. Deployment can be on the electric power pole, pad-mount transformer station, street cabinet, or in the network room of an MDU building. Please note that the gateway is IP65 compliant, so if it is to be installed outdoors, it should be placed in another cabinet to protect it from heavy rain. It can be easily mounted on walls or hanged on wires. Grounding the case is recommended for safety, and should be done according to the local electric code of conduct. See figure below for installation example.

The devices can be powered by AC or DC.

The LV and HD Compact Gateways have a waterproof connector interface to transfer the BPL signal through the low voltage wire in the same socket as the feeding power. There is a separated socket from the power plug providing interfaces to 4 wires (three phase lines and one neutral line). There is also an alternative to use the provided coaxial interface to inject or couple the BPL signal into the power line wires by an external coupler. To inject the BPL signal into a Medium-Voltage or any voltage higher than 270 Volts, a proper external coupler must be used. The Ethernet port is provided in a protective waterproof connector attached to the housing allowing a direct access to the device. See figure below.

Figure 1: Waterproof RJ45 connector for local Ethernet access

CONNECTING AND POWERING THE LV AND HD COMPACT GATEWAY

The LV and HD Compact Gateways come with a waterproof 4-pin male connector for BPL signal and feeding power. A matching female socket connector is provided in the package.

Figure 2: AC Pin configurations on the Gateway

Figure 3: AC Pin configurations on the Cable

Figure 4: DC Pin configurations on the Gateway

Figure 5: DC Pin configurations on the Cable

	1	2	3	4
AC	Phase A (Brown/Yellow)	Phase B (Black)	Phase 3 (Grey / White)	Neutral (Blue)
DC	GND	NC	Bt in ⊕ 14.4V	+12V Out

The figure below shows an example of using conductive couplers on a three-phase, four-wire system.

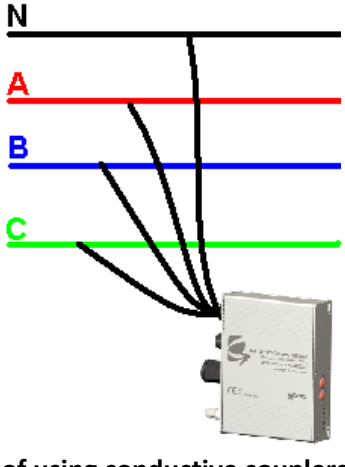


Figure 6: Example of using conductive couplers for 3-phase lines

In some deployments, the Gateway can communicate with other modems over a coaxial cable or injecting the BPL signal into the power line by using an external coupler that comes with coaxial interface, for example Corinex Coaxial to Powerline Coupler (CXZ-CXC-PH2)or Corinex 11+1 Coupler (CXZ-CXC-PH12). A proper configuration settings file must be loaded into the Gateway to direct the BPL signal to coaxial rather than LV output. Connectivity over the coaxial cable is always better than the power line. However, to obtain a maximum performance, high performance and low loss cable like RG-6 type is preferred. Either 50-ohm or 75-ohm impedance can be used with the coaxial interface. Impedance matching between coaxial cable and the connector is insignificant and the throughput impairment from mismatching impedance is negligible.

Figure 7: Signal output ports and power connector (Coax, Ethernet, DC, AC)

CONNECTING THE AC WIRE

Pin 1	Brown/Yellow	AC Line 1	AC Power Line PLC +
Pin 2	Black	AC Line 2	PLC +
Pin 3	Grey/White	AC Line 3	PLC +
Pin 4	Blue	Neutral	AC Power Neutral PLC -

BUTTON AND LEDS

Buttons

Each of the two buttons has multiple functionalities. The functions will change depending on how long it is pressed. The table below describes the functionalities:

Button	Indication	1st function press from 1 to 4 seconds	2nd function press for 10 seconds
RST	N/A	Hardware reset	Factory-default reset
CP-SW	LV-C	Switch coupling mode (LV / Coax) **Optional A**: Switch MAC (PLC / EoC) **Optional B**: Switch RPM (enable / disable)	Switch PTTP mode (enabled/ disable)

Note: In the default configuration, the ability to switch MAC and RPM is disabled. In order to enable these functionalities, a configuration update in NVRAM using SNMP is necessary. After this update, the 1st function of BTN-2 will switch option A and B at once (MAC switch to PLC and RPM switch to enabled; MAC switch to EoC and RPM switch to disabled).

LEDS

Each of the 6 LEDs helps to show and diagnose the behavior of the gateway. In some cases, multiple states are displayed by one LED.

		State			
LED	**Function**	**On**	**Off**	**Alternate 1s**	**Alternating 0.1s**
PWR	Power	Power ON	Power OFF	NA	NA
LV-C*	- Coupling Mode (1st function) - PTTP Mode (2nd function)	Coupling to LV **Optional A**: RPM enabled	Coupling to COAX **Optional A**: RPM disabled	NA	Blinking period to indicate PTTP
REG	- Auto Configuration - Pushbutton (1st and 2nd function)	Auto Configuration is done	-Auto Configuration is not finished -IP is not set	-Auto Configuration is not finished -IP is assigned	Blink from 1s to 4s and after 8s while button is being pressed
ETH	ETH L/A	Eth link established	No Eth link/ETH10 Speed	NA	There is Eth activity
DC-PWR	DC Power	DC Power ON	DC Power OFF	NA	NA
PLC	PLC L/A + Port solver	PLC link established	No device connected to port solver	Some devices are connected to port solver	There is PLC activity

- * Indicating PTTP mode
  - **If PTTP Mode is Disabled**
    - **LV-C** will only indicate Coupling Mode (On for LV, Off for COAX)
  - **If PTTP Mode is Enabled**
    - **LV-C** will alternate between indicating Coupling Mode and PTTP Mode**:**
      - For 5s – it indicates Coupling Mode (On for LV, Off for COAX)
      - For 2s – it indicates PTTP is enabled by alternating every 0.1s
      - This 2 stats will cycle

DEFAULT CONFIGURATION SETTINGS

Zero Cross Dection GPIO -4	Zero Cross Dection is not available
Notch	Enabled
Encryption	Disabled
PTTP mode	Enabled
Admin password Config	Default telnet Admin mode password: maxibon Admin password should be configurable through telnet command
SNMP community name in Telnet	Admin mode, section SNMPReadWrite information i Information about SNMP community names change c Change read or write community name Usage: <[r|w]> <oldname> <newname> The length of community name should be 3~10 characters inclusively
Telnet console password	Adminpasswdset apass Set mode admin password Usage: apass <old_password> <new_password> The length of password should be 3~10 characters inclusively
Coupling Mode	Default LV. Can be switched by the push button, Telnet, SNMP, or the auto-config file
Push button	See above section on buttons
Telnet	Admin mode, section SwitchPlcCoax information i Information about the current coupling mode set s Couple PLC signal to LV or Coax Usage s [LV|COAX]
SNMP	iso.3.6.1.4.1.6798.3.20.3.1.1.2.1 rw Couple PLC signal to LV or Coax LV => 0, COAX => 1
Auto Config File	PLC_SIGNAL_COUPLING = [LV | COAX]
EXTA interface	Default enabled. Can be switched by Telnet, SNMP, or the auto-config file
Telnet	Admin mode, section ExtA information i Show all MACs for the port EXTA Usage: i <i> EXTA e Enable/Disable interface EXTA Usage: e <e|d>
SNMP	iso.3.6.1.4.1.6798.3.20.2.1.1.2.1 rw Enable/disable interface EXTA Enable => 0, Disable => 1
Auto Config File	DISABLE_EXTA = [yes|no]
Show all MACs for port EXTA	Can be switched by Telnet and SNMP
Telnet	Admin mode, section ExtA information i Show all MACs for the port EXTA Usage: i <i>
SNMP	iso.3.6.1.4.1.6798.3.20.1 r Show all MACs for port EXTA. Use walk function
Web Interface	Enabled (read only)
Ability to switch MAC Mode by PushButton	Default disabled. Can be switched by SNMP
SNMP	iso.3.6.1.4.1.6798.3.20.3.1.1.3.1 rw Enable/disable to control switching MAC to PLC or EoC by PushButton Enable => 0, Disable => 1
Ability to switch RPM Mode by PushButton	Default disabled. Can be switched by SNMP.
SNMP	iso.3.6.1.4.1.6798.3.20.3.1.1.4.1 rw Enable/disable control RPM to enable/disable by PushButton Enable => 0, Disable => 1

FIRMWARE AND DEVICE STRUCTURE

Corinex LV and HD Compact Gateways are built on AV200 technology which is capable to reach physical throughput of up to 200 Mbps. The line driver of the Gateway is powerful and robust, and can be used as a Head-End Master (HE), Time Division Repeater (TDR), or Slave (CPE) unit depending on the configuration settings.

There are 3 functions of the BPL device in network hierarchy. HE unit is a Master modem in a BPL network controlling traffic and connection negotiation from TDR or CPE units in the same power line coverage. A CPE unit can connect directly to the HE unit or through TDR unit depending on the configuration setting options. TDR units have a main function to extend the coverage over longer distance or increase the number of end users. TDR units behave as a Slave for the Master unit and as a Master for the Slave unit. Channel access on the BPL media is controlled mainly from the Master unit by token passing. The TDR unit also controls channel access for its Slave units by forwarding the token received from its Master unit.

In a BPL network, there should only be one HE unit. To have more than one HE master modem in the same power line coverage, Frequency Division scheme must be used by setting each HE unit to run a different frequency mode. Corinex Enterprise firmware provides a solution to use 3 different equal frequency bands; Mode 1, Mode 2, and Mode 3.

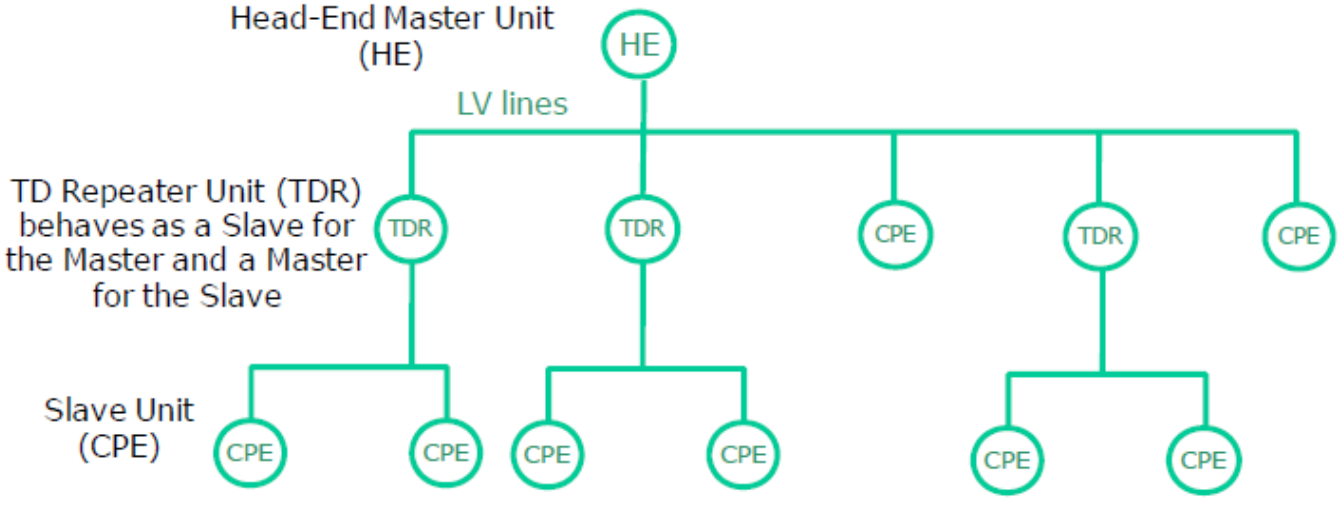


Figure 8: Typical BPL Network Hierarchy

All Gateway models are running Corinex Enterprise firmware and are set to run the auto-configuration boot-up process by default. This process requires DHCP and TFTP server to provide the network settings and configuration file to the modem.

The modem has a command line interface console for changing configuration and checking status of its operation or connectivity with the other modems. A number of parameters can be defined in an auto-configuration file stored in the TFTP server. When the modem requests an IP from the DHCP server, it will be provided with an instruction to download a configuration file from TFTP server together with the assigned IP address using BOOTP protocol. The text file below shows a simple auto-configuration file for the HE unit:

```
GENERAL_USE_AUTOCONF = YES
```

GENERAL_TYPE = HE
GENERAL_FW_TYPE = LV
GENERAL_IP_ADDRESS = 10.10.1.100
GENERAL_IP_NETMASK = 255.255.255.0
GENERAL_IP_GATEWAY = 10.10.1.1
GENERAL_IP_USE_DHCP = YES
GENERAL_STP = YES
GENERAL_AUTHENTICATION = NONE
GENERAL_SIGNAL_MODE = 6
SIGNAL_SUB_MODE = 0
GENERAL_SIGNAL_REG_POWER_MASK_ENABLE = NO
PLC_SIGNAL_COUPLING = LV
MCAST_MPP2IGMP_PORT = NONE
MCAST_IGMP_SNOOPING = NO

By default the modem with Enterprise firmware is running as a CPE unit searching all possible frequency modes for the BPL signal from the connecting line. If the Gateway is running by the above configuration file and connecting to other modems on the same physical line, they should make a connection and show the connectivity status in the master modem's CLI console similar to the below figure.

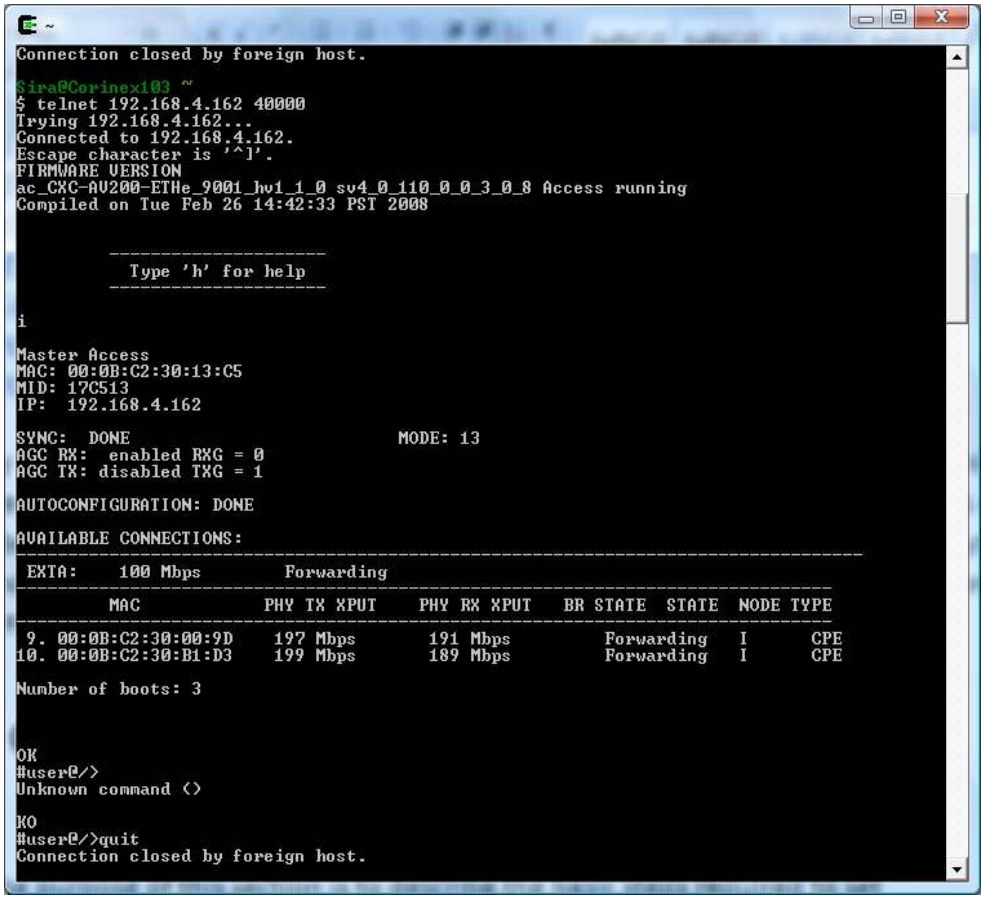
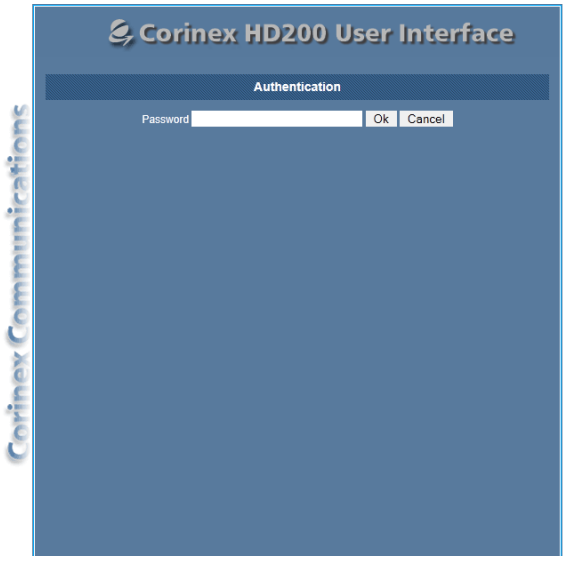


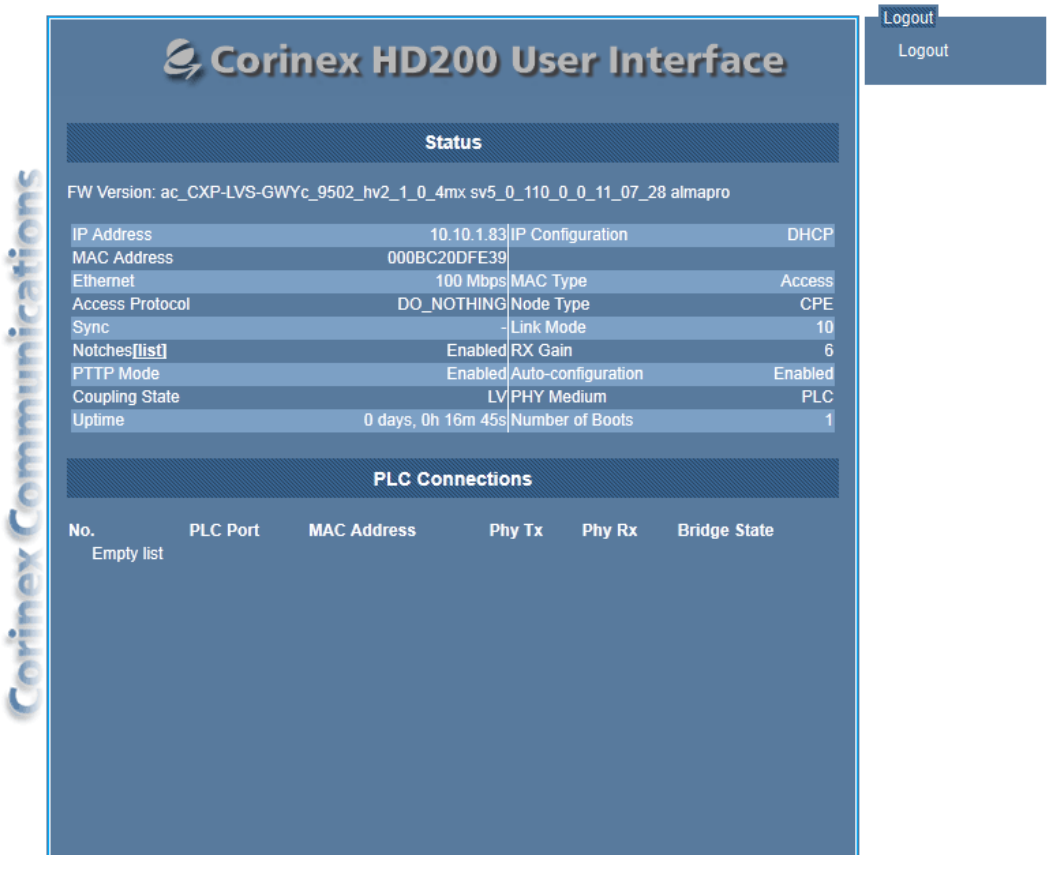
Figure 9: CLI console from Telnet showing connectivity status

Web Interface

The web interface can be accessed by entering the IP-Address of the gateway into a web browser. The default password is **paterna**.



The web interface makes it easy to view the current settings of a gateway and monitor its status.


Logout
Logout
Corinex HD200 User Interface
Status
FW Version: ac_CXP-LVS-GWYc_9502_hv2_1_0_4mx sv5_0_110_0_0_11_07_28 almapro
IP Address 10.10.1.83 IP Configuration DHCP
MAC Address 000BC20DFE39
Ethernet 100 Mbps MAC Type Access
Access Protocol DO_NOTHING Node Type CPE
Sync - Link Mode 10
Notches[list] Enabled RX Gain 6
PTTP Mode Enabled Auto-configuration Enabled
Coupling State LV PHY Medium PLC
Uptime 0 days, 0h 16m 45s Number of Boots 1
PLC Connections
No. PLC Port MAC Address Phy Tx Phy Rx Bridge State
Empty list
Corinex Communications

CONFIGURATIONS AND SETTINGS

Preparing DHCP/TFTP server

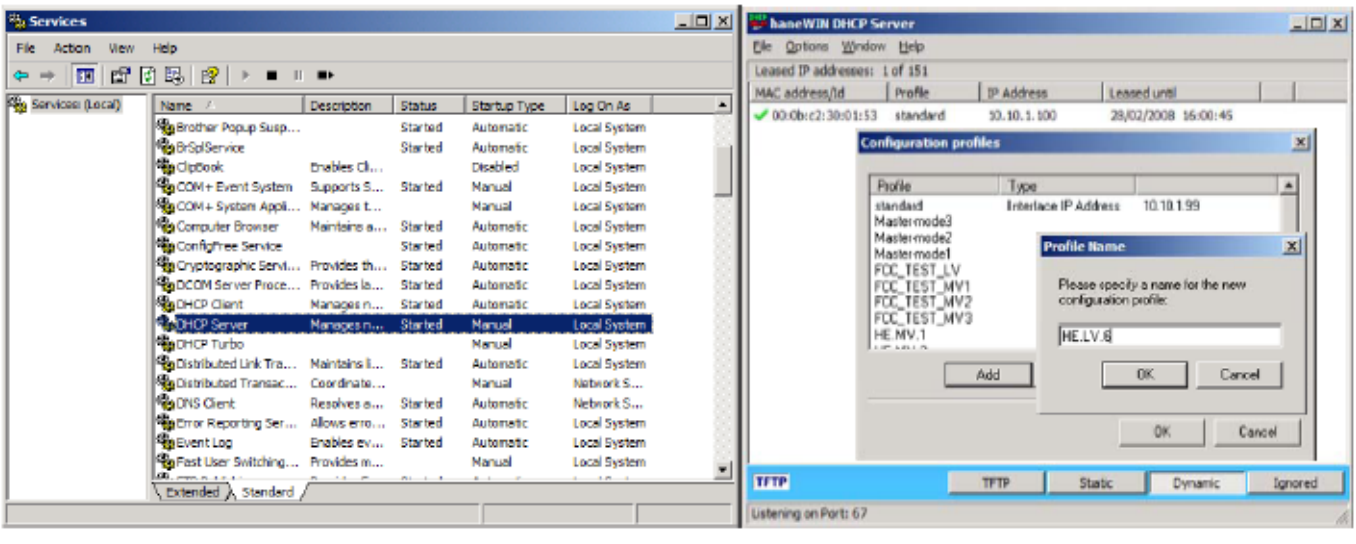
The following steps are for installing and preparing DHCP server on a PC. After running this procedure, the DHCP/TFTP server will be set up properly in the PC and there is no need to run the procedure again.

Step 1: Turning off Windows Firewall from the Control Panel

To configure an AV200 modem, a number of UDP and TCP ports in Windows are used by the DHCP/TFTP server and other applications. Therefore, those ports must be allowed by Windows firewall or the firewall must be turned off. If the PC is running any anti-virus software and those ports are protected by anti-virus, that feature should be disabled according to the antivirus documentation.

If Window Firewall cannot be turned off, the following ports must be allowed for those applications.

- UDP port 68 used by BOOTPC
- UDP port 67 used by BOOTPS
- UDP port 69 used by TFTP

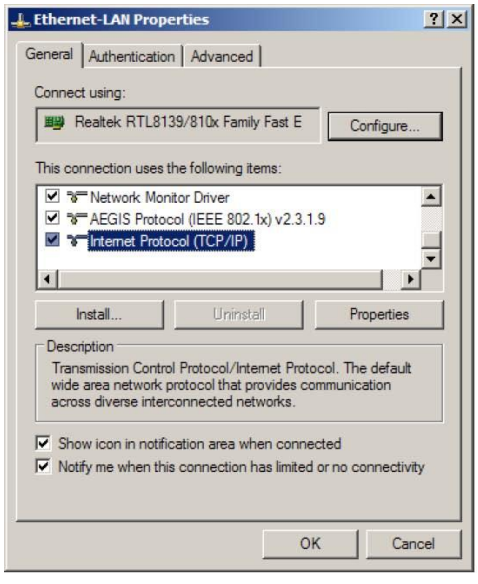


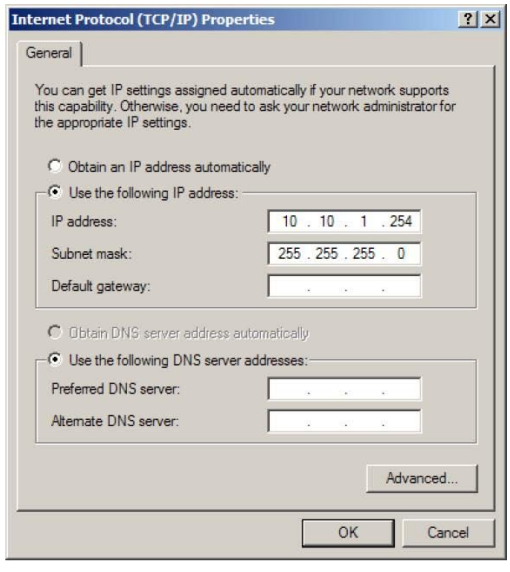
Step 2: Installing DHCP server

This document is using haneWIN DHCP Server 3.0.18 for illustration. Any other DHCP server or later version of haneWIN can also be used by following the instruction of the respective DHCP server and applying the similar settings. DHCP servers that can be used with auto-configuration must support BOOTP protocol. The user can download DHCP server from www.hanewin.de and install in the PC. The unregistered version can be used up to 30 days. Later version supports Windows Vista™.

Step 3: Preparing the network interface on the PC

The PC network interface must have a fix IP address set in order to use the DHCP server on the PC. In our example the IP address 10.10.1.254 and subnet 255.255.255.0 are used.




Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 10 . 1 . 254
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

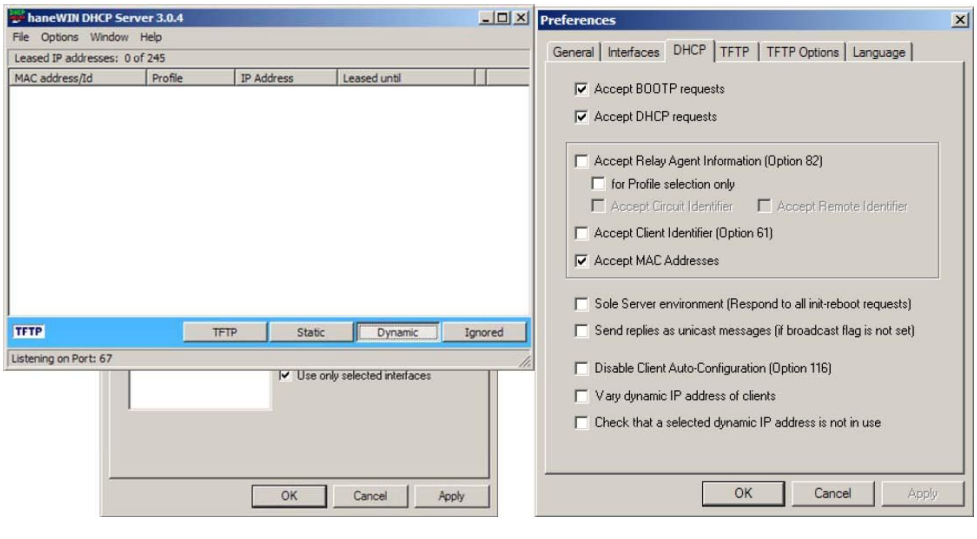
This can also be done by the Windows command line (C:\WINDOWS\system32\cmd.exe) and executing “netsh” with the following parameters.

>netsh interface ip set address "Ethernet-LAN" static 10.10.1.254 255.255.255.0

Network interface named “Ethernet-LAN” might be different. To check the correct name, the user can use “ipconfig” to display all Ethernet interfaces in the PC.

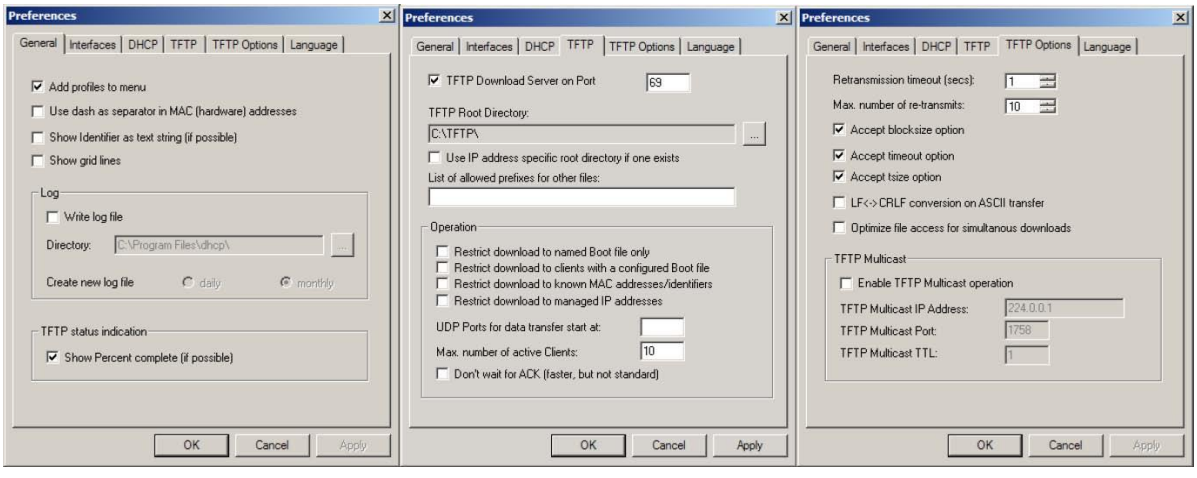
Step 4: Setting a default interface for DHCP server

The user must activate DHCP server from File > Service > Activate. This will run DHCP server as a Windows service. The user can check and verify that this service has been started from Services in Administrative Tools. By default, haneWIN will start automatically after Windows started. To prevent from automatic starting, the user can set it to start manually. If the Ethernet interface is active, it will show on the preference tab. Interface 10.10.1.254 must be checked, other interface shown must be clear, and ‘Use only selected interfaces’ must be checked to prevent the other network interface from using this DHCP server.



The user can use TFTP server that comes with haneWIN DHCP. TFTP has a root directory where all auto-configuration files shall be located. Make sure that this root directory is customized properly and all *.conf

are copied to this root directory. Otherwise, TFTP server won't be able to find the requested file.

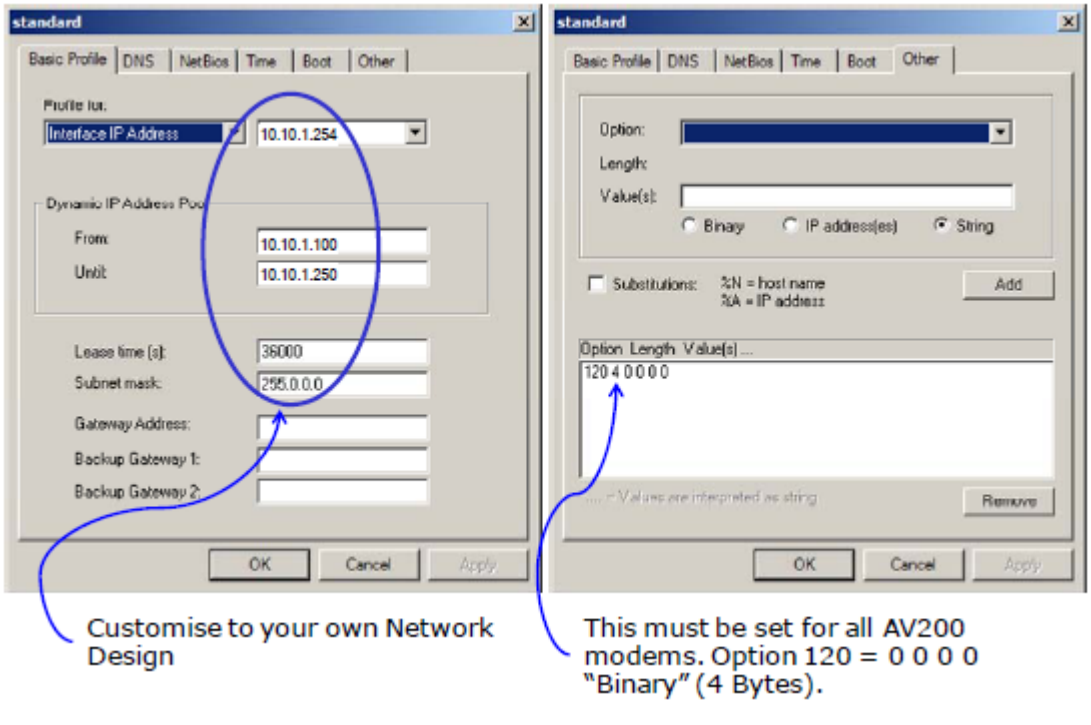


Step 5: Setting a standard profile for DHCP server

DHCP server will set a default standard profile for the selected IP interface from step 3. This must be customized for the network to be used with AV200 modems. The following setting set this interface to provide IP addresses ranging from 10.10.1.100 to 10.10.1.250 to any requested client with subnet mask 255.0.0.0. AV200 modem needs additional setting on Option 120 to be binary 0 0 0 0 or unsigned 32-bit integer 0x0000.

The figure below shows the applied settings:

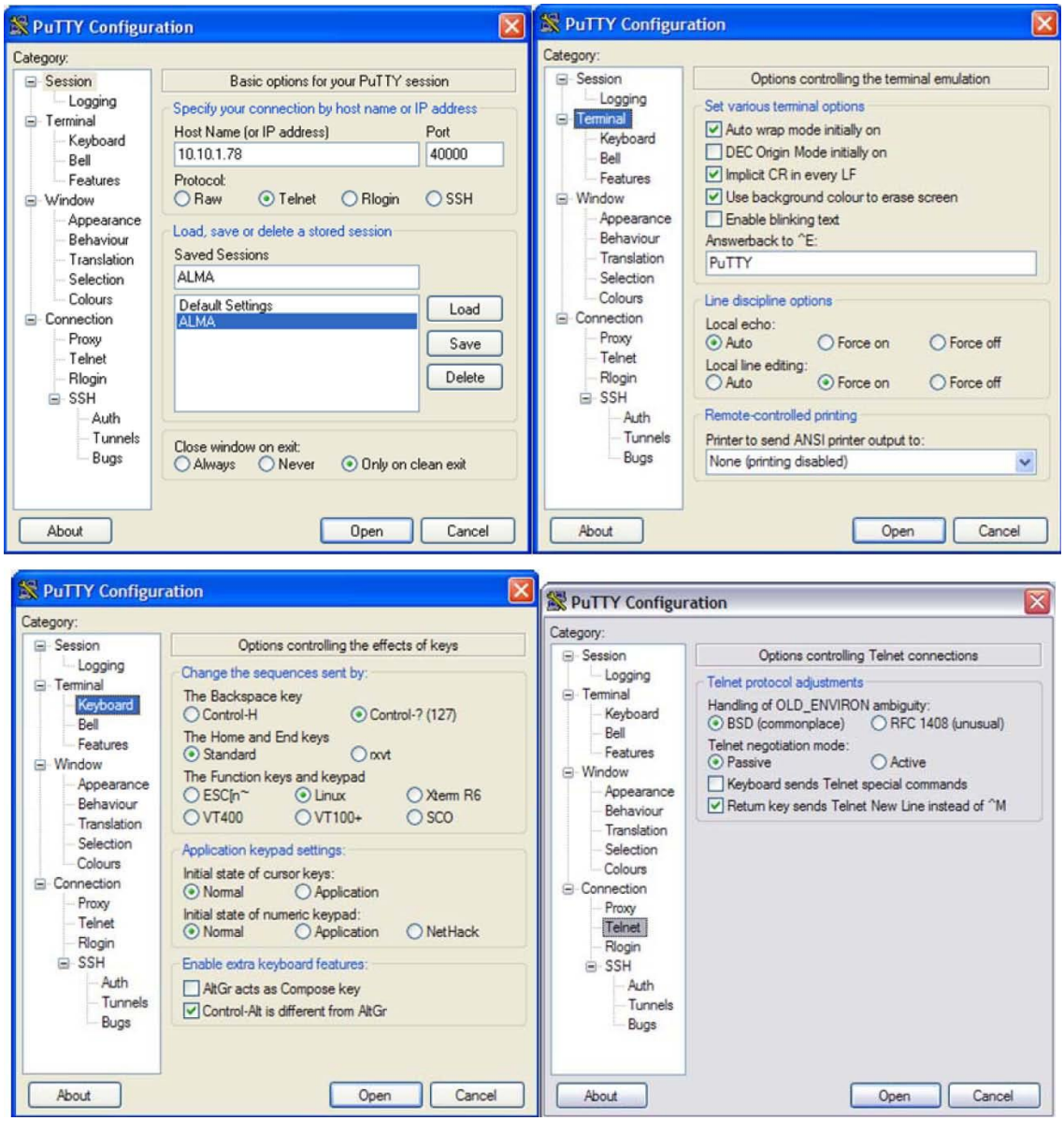
- Interface IP = 10.10.1.254
- Dynamic IP address pool from 10.10.1.100 to 10.10.1.250
- Any lease time and subnet mask is OK.
- Option 120 gives value of binary "0 0 0 0". Make sure that after adding, it shows "120 4 0 0 0 0".



Preparing Telnet PuTTY for command line interface (CLI) console

AV200 modem needs a Telnet client running on a PC to interface, monitor, and control all the functions available for command line interfaces (CLI). Telnet client should have the following settings:

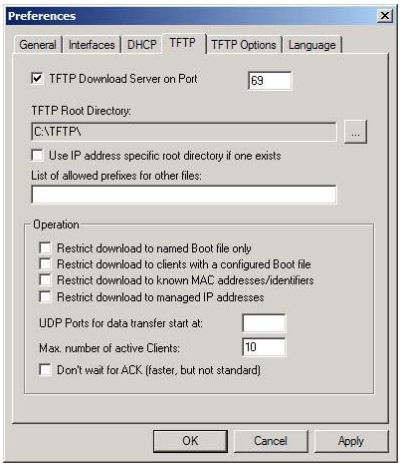
- Telnet port 40000
- CR/LF
- Local echo on and local line editing on
- Best for Linux terminal and compatible with VT100 terminal
- Passive Telnet negotiation mode (send after CR allowing Backspace to correct the mistype.)
- Login admin mode by /mode admin and password “maxibon” (PuTTY needs login twice.)
- Common commands used in CLI are ‘l’ and ‘ls’.



Loading auto-configuration file (*.conf)

Step 1: Preparing an auto-configuration file

In TFTP server setup, the root directory must be specified and this is the folder for all auto-configuration files with .conf extension. Auto-configuration file is a simple text file edited by a text editor (e.g. Notepad) to set up each AV200 modem.



A simple configuration for a master modem is as follows. In our example, it must be saved in file HE.LV.6.conf.

```
GENERAL_USE_AUTOCONF = YES
GENERAL_TYPE = HE
GENERAL_FW_TYPE = LV
#GENERAL_IP_ADDRESS = 10.10.1.105
#GENERAL_IP_NETMASK = 255.255.255.0
#GENERAL_IP_GATEWAY = 10.10.1.1
GENERAL_IP_USE_DHCP = YES
GENERAL_STP = YES
GENERAL_AUTHENTICATION = NONE
GENERAL_SIGNAL_MODE = 6
GENERAL_SIGNAL_REG_POWER_MASK_ENABLE = NO
PLC_SIGNAL_COUPLING = LV
```

Below is a simple configuration for slave modem using Corinex AV200 Enterprise Powerline Adapter.

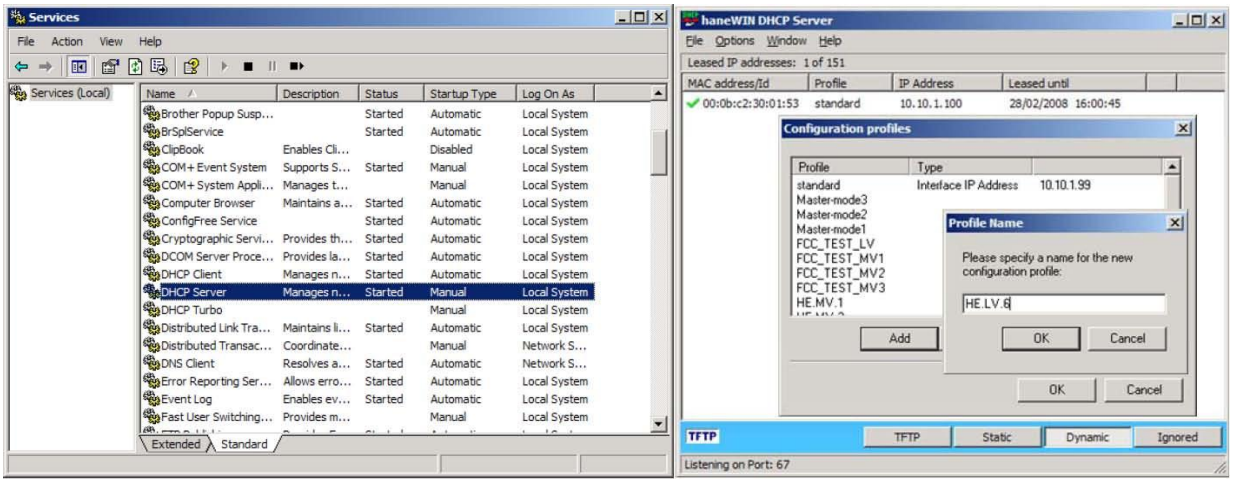
```
GENERAL_USE_AUTOCONF = YES
GENERAL_TYPE = CPE
GENERAL_FW_TYPE = LV
#GENERAL_IP_ADDRESS = 10.10.1.105
#GENERAL_IP_NETMASK = 255.255.255.0
#GENERAL_IP_GATEWAY = 10.10.1.1
GENERAL_IP_USE_DHCP = YES
GENERAL_STP = YES
GENERAL_SIGNAL_REG_POWER_MASK_ENABLE = NO
```

The master modem needs to download a configuration file from TFTP server in order to work properly. But the slave modem doesn't need a configuration file as it is set to CPE type by default. If there is a special

setting for the slave modem, it can be included in slave or CPE configuration (for example signal_mode_list).

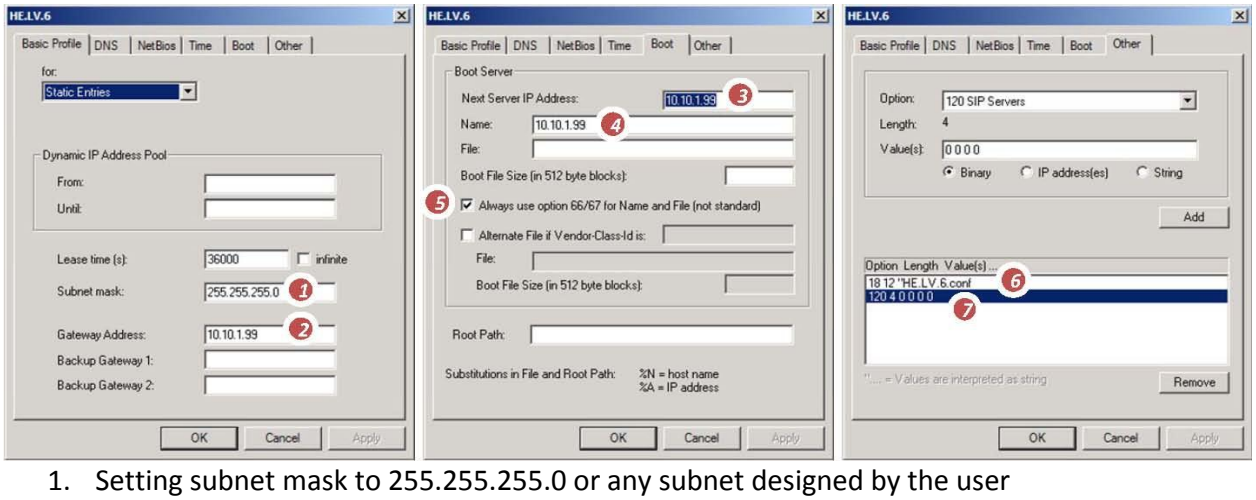
Step 2: Preparing a DHCP profile to download auto-configuration

To prepare a profile in DHCP server, the user must make sure that DHCP server is running. In Windows services, the "DHCP server" must have a status of "started".



In DHCP server, under Options, Manage Profiles, and Add, a profile name will be requested. This name can be chosen by the user. Any name that can refer to the function of the modem is applicable. For example, "HE.LV.6" would mean Head End (master) on LV access MAC mode running on mode 6.

To set up a profile, the user must specify the following options:

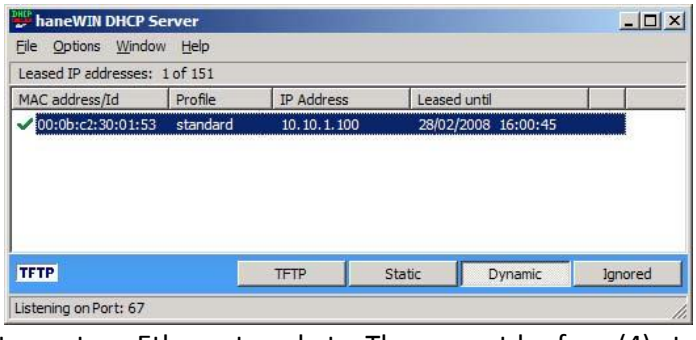


1. Setting subnet mask to 255.255.255.0 or any subnet designed by the user
2. Setting gateway address to this PC
3. Setting TFTP server address
4. Setting TFTP name, must be a TFTP address
5. Setting option 66
6. Setting option 18 to auto-configuration file name with .conf extension (string)
7. Setting option 120 to '0 0 0 0', 4 zeros and 3 spaces (binary)

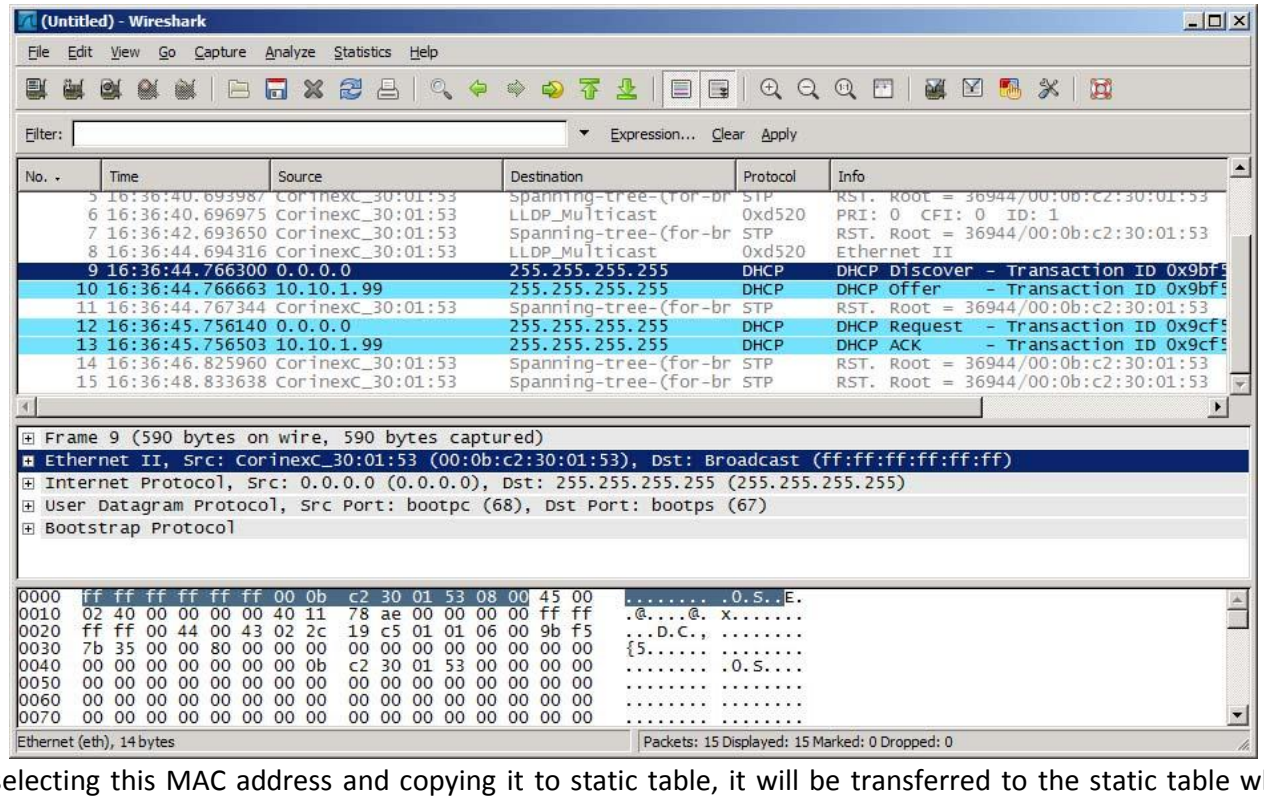
Then this profile is ready for the next step.

Step 3: Binding a DHCP profile with static IP table

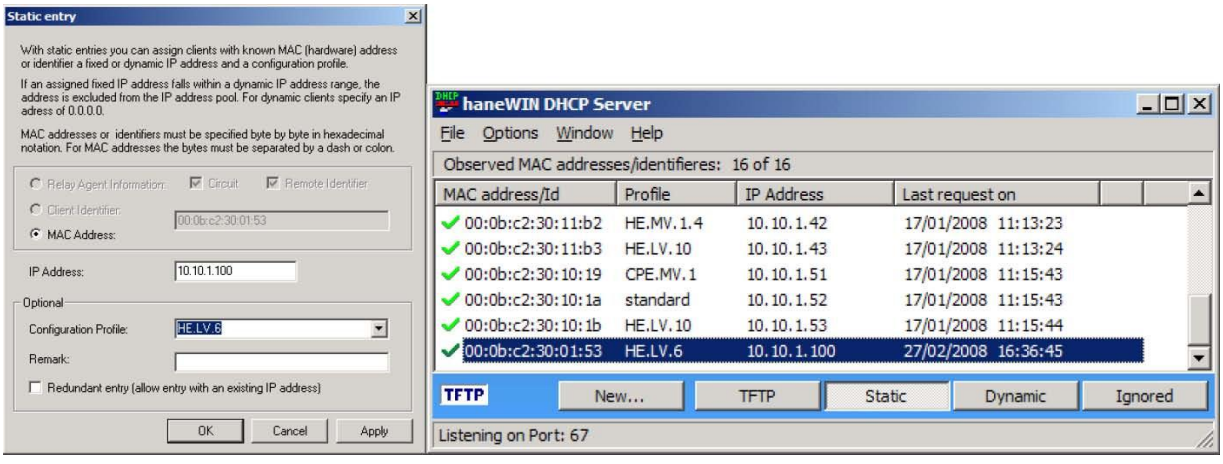
In this step, the modem must connect to a PC and get an IP from the DHCP server. The MAC address of the modem will appear (1 MAC address for a single modem and 3 MAC addresses for MDU or MV Gateway), in DHCP dynamic table.


haneWIN DHCP Server
File Options Window Help
Leased IP addresses: 1 of 151
MAC address/Id Profile IP Address Leased until
00:0b:c2:30:01:53 standard 10.10.1.100 28/02/2008 16:00:45
TFTP
TFTP Static Dynamic Ignored
Listening on Port: 67

The user can use Ethereal to capture Ethernet packets. There must be four (4) steps of DHCP request; DHCP discovery, offer, request, and ack. If there is no response from the server (10.10.1.99), then there must be something wrong with the server setting. The user must check Basic Procedure 1 again.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
6 16:36:40.696975 CorinexC_30:01:53 LLDP_Multicast 0xd520 PRI: 0 CFI: 0 ID: 1
7 16:36:42.693650 CorinexC_30:01:53 Spanning-tree-(for-br STP RST. Root = 36944/00:0b:c2:30:01:53
8 16:36:44.694316 CorinexC_30:01:53 LLDP_Multicast 0xd520 Ethernet II
9 16:36:44.766300 0.0.0.0 255.255.255.255 DHCP DHCP Discover - Transaction ID 0x9bf5
10 16:36:44.766663 10.10.1.99 255.255.255.255 DHCP DHCP Offer - Transaction ID 0x9bf5
11 16:36:44.767344 CorinexC_30:01:53 Spanning-tree-(for-br STP RST. Root = 36944/00:0b:c2:30:01:53
12 16:36:45.756140 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x9cf5
13 16:36:45.756503 10.10.1.99 255.255.255.255 DHCP DHCP ACK - Transaction ID 0x9cf5
14 16:36:46.825960 CorinexC_30:01:53 Spanning-tree-(for-br STP RST. Root = 36944/00:0b:c2:30:01:53
15 16:36:48.833638 CorinexC_30:01:53 Spanning-tree-(for-br STP RST. Root = 36944/00:0b:c2:30:01:53
Frame 9 (590 bytes on wire, 590 bytes captured)
Ethernet II, Src: CorinexC_30:01:53 (00:0b:c2:30:01:53), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
0000 ff ff ff ff ff ff 00 0b c2 30 01 53 08 00 45 00 ..... .0.S..E.
0010 02 40 00 00 00 00 40 11 78 ae 00 00 00 00 ff ff .@....@. x.....
0020 ff ff 00 44 00 43 02 2c 19 c5 01 01 06 00 9b f5 ...D.C., ...
0030 7b 35 00 00 80 00 00 00 00 00 00 00 00 00 00 00 {5..... .....
0040 00 00 00 00 00 00 00 0b c2 30 01 53 00 00 00 00 ..... .0.S....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
Ethernet (eth), 14 bytes
Packets: 15 Displayed: 15 Marked: 0 Dropped: 0

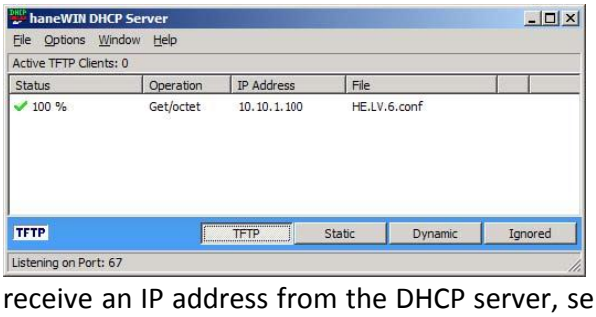
By selecting this MAC address and copying it to static table, it will be transferred to the static table which allows the user to bind it with any IP and profile. If the user changes IP address, the old address must be deleted from the dynamic table to avoid duplication. Configuration profile is the profile to instruct this modem to download an auto-configuration file from TFTP server, in this example HE.LV.6.conf.


Static entry
With static entries you can assign clients with known MAC (hardware) address or identifier a fixed or dynamic IP address and a configuration profile.
If an assigned fixed IP address falls within a dynamic IP address range, the address is excluded from the IP address pool. For dynamic clients specify an IP adress of 0.0.0.0.
MAC addresses or identifiers must be specified byte by byte in hexadecimal notation. For MAC addresses the bytes must be separated by a dash or colon.
Relay Agent Information
Circuit
Remote Identifier
Client Identifier:
MAC Address:
00:0b:c2:30:01:53
IP Address:
10.10.1.100
Optional
Configuration Profile:
HE.LV.6
Remark:
Redundant entry (allow entry with an existing IP address)
OK
Cancel
Apply
haneWIN DHCP Server
File Options Window Help
Observed MAC addresses/identifieres: 16 of 16
MAC address/Id
Profile
IP Address
Last request on
00:0b:c2:30:11:b2 HE.MV.1.4 10.10.1.42 17/01/2008 11:13:23
00:0b:c2:30:11:b3 HE.LV.10 10.10.1.43 17/01/2008 11:13:24
00:0b:c2:30:10:19 CPE.MV.1 10.10.1.51 17/01/2008 11:15:43
00:0b:c2:30:10:1a standard 10.10.1.52 17/01/2008 11:15:43
00:0b:c2:30:10:1b HE.LV.10 10.10.1.53 17/01/2008 11:15:44
00:0b:c2:30:01:53 HE.LV.6 10.10.1.100 27/02/2008 16:36:45
TFTP
New...
TFTP
Static
Dynamic
Ignored
Listening on Port: 67

After completely binding a profile to the IP address, on the static IP table, it shows the correct profile to be used.

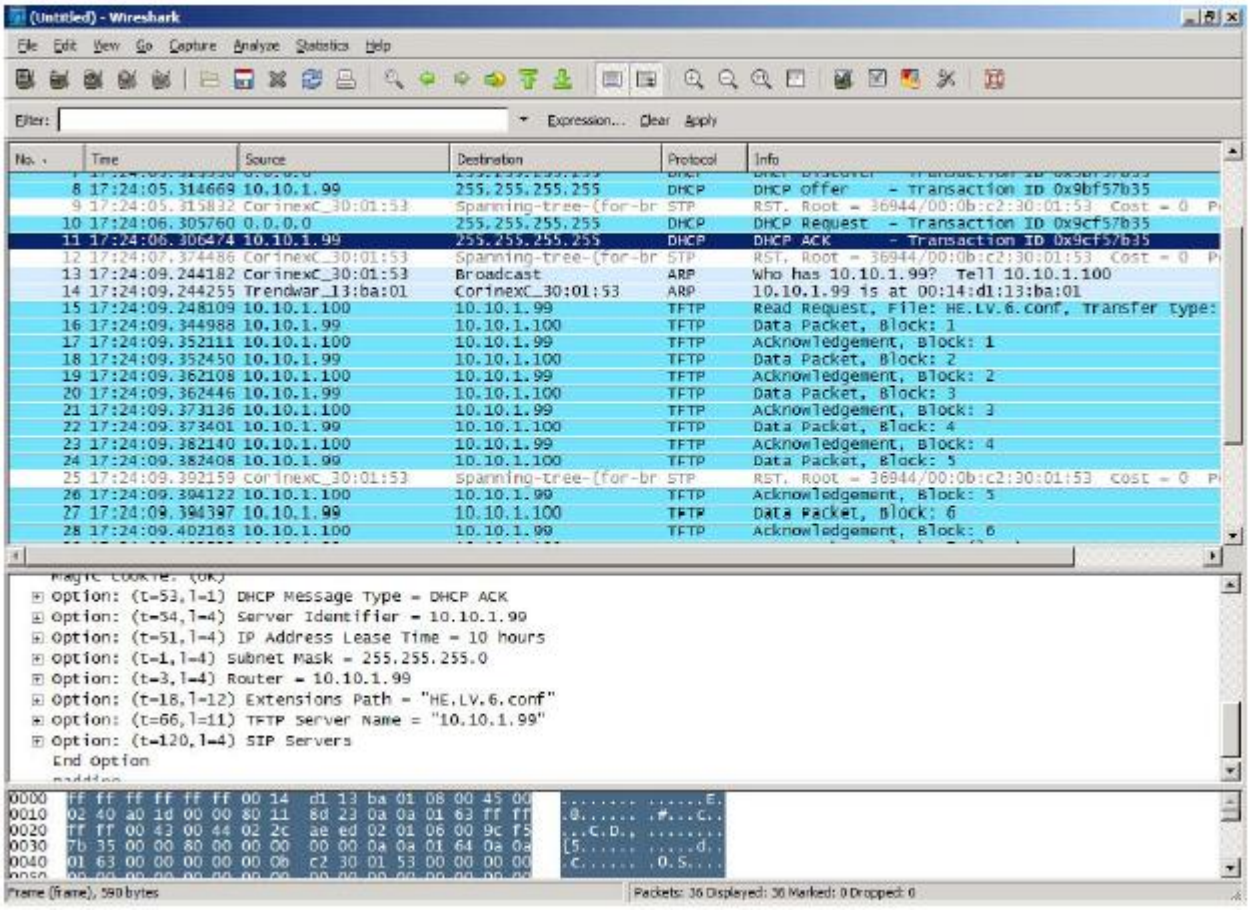
Step 4: Rebooting the modem and checking the loading process

As changes in the DHCP server are done, after the modem gets an IP address, the modem won't reload the configuration until it is either reset, factory reset, rebooted, or the IP lease time has ended. The user must reboot the modem by powering it off and on again. The Power switch on the MDU gateway will turn on and off all 3 modules at the same time. If the user want to reset only one modem, the use must telnet and log in as an Admin and use the command "/hw rst" for reset or "/frst frst" for factory reset. In an older firmware (version 3), factory reset command is "/hw frst".



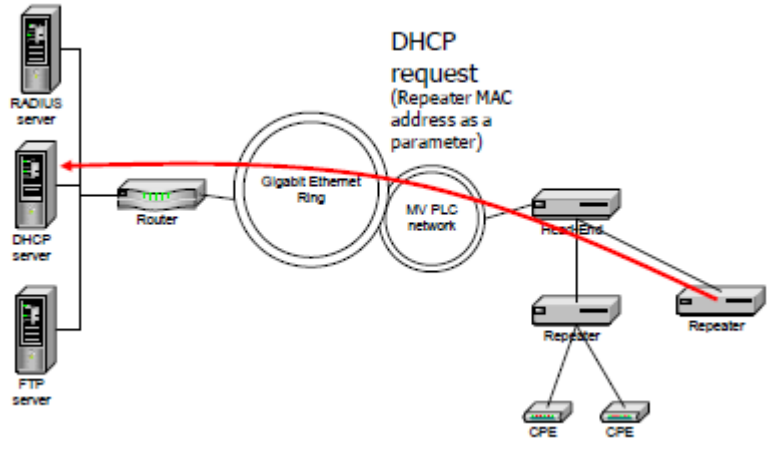
After reboot, the modem shall receive an IP address from the DHCP server, send a request for file download to the TFTP server, and download the *.conf file from the server. In the Ethereal capture below, it shows the process of DHCP and TFTP download. There are 4 DHCP steps: discover, offer, request, and acknowledge (ack). On offer and ack steps, the DHCP server includes 4 options in the message. Option 3 is a gateway IP. Option 18 is the configuration filename. Option 66 is the TFTP server IP address. And Option 120 is to turn off management VLAN. If any of those options is missing, the modem won't properly load the configuration file from the server. It is recommended to keep monitoring using Ethereal in order to prevent any mistakes. The user can check the content of *.conf file in the data packets.

On Ethereal, the user must see packets containing Rapid Spanning Tree Protocol (BPDU) sent out from the modem through Ethernet port from time to time. If the user cannot see RSTP BPDU or there is a VLAN tag on this packet, then there is something wrong with the DHCP setting or modem.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
8 17:24:05.314669 10.10.1.99 255.255.255.255 DHCP DHCP Offer - Transaction ID 0x9bf57b35
10 17:24:06.305760 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x9cf57b35
11 17:24:06.306474 10.10.1.99 255.255.255.255 DHCP DHCP ACK - Transaction ID 0x9cf57b35
13 17:24:09.244182 CorinexC_30:01:53 Broadcast ARP Who has 10.10.1.99? Tell 10.10.1.100
14 17:24:09.244255 Trendwar_13:ba:01 CorinexC_30:01:53 ARP 10.10.1.99 is at 00:14:d1:13:ba:01
15 17:24:09.248109 10.10.1.100 10.10.1.99 TFTP Read Request, File: HE.LV.6.conf, Transfer type:
16 17:24:09.344988 10.10.1.99 10.10.1.100 TFTP Data Packet, Block: 1
17 17:24:09.352111 10.10.1.100 10.10.1.99 TFTP Acknowledgement, Block: 1
18 17:24:09.352450 10.10.1.99 10.10.1.100 TFTP Data Packet, Block: 2
19 17:24:09.362108 10.10.1.100 10.10.1.99 TFTP Acknowledgement, Block: 2
20 17:24:09.362446 10.10.1.99 10.10.1.100 TFTP Data Packet, Block: 3
21 17:24:09.373136 10.10.1.100 10.10.1.99 TFTP Acknowledgement, Block: 3
22 17:24:09.373401 10.10.1.99 10.10.1.100 TFTP Data Packet, Block: 4
23 17:24:09.382140 10.10.1.100 10.10.1.99 TFTP Acknowledgement, Block: 4
24 17:24:09.382408 10.10.1.99 10.10.1.100 TFTP Data Packet, Block: 5
26 17:24:09.394122 10.10.1.100 10.10.1.99 TFTP Acknowledgement, Block: 5
27 17:24:09.394397 10.10.1.99 10.10.1.100 TFTP Data Packet, Block: 6
28 17:24:09.402163 10.10.1.100 10.10.1.99 TFTP Acknowledgement, Block: 6
Option: (t=53,l=1) DHCP Message Type = DHCP ACK
Option: (t=54,l=4) Server Identifier = 10.10.1.99
Option: (t=51,l=4) IP Address Lease Time = 10 hours
Option: (t=1,l=4) Subnet Mask = 255.255.255.0
Option: (t=3,l=4) Router = 10.10.1.99
Option: (t=18,l=12) Extensions Path = "HE.LV.6.conf"
Option: (t=66,l=11) TFTP Server Name = "10.10.1.99"
Option: (t=120,l=4) SIP Servers
End Option

Step 5: Loading auto-configuration files to other modems

The user doesn't need to connect PC to all adapters or modems directly in the network to load a configuration file. After the first modem connected directly to the PC loaded its configuration, it will restart and turn into a master modem which allows all other modems to connect to. Then, the other connecting modem will broadcast DHCP offer and request IP address through BPL channel to the master modem's Ethernet port. The same process will be taken in the sequential order until the last modem.



EXAMPLE OF DEPLOYMENT

The first example of deployment shows a typical application for the last mile access to servicing houses from GPON optical fiber cable end or an Internet access end point via UTP cable.

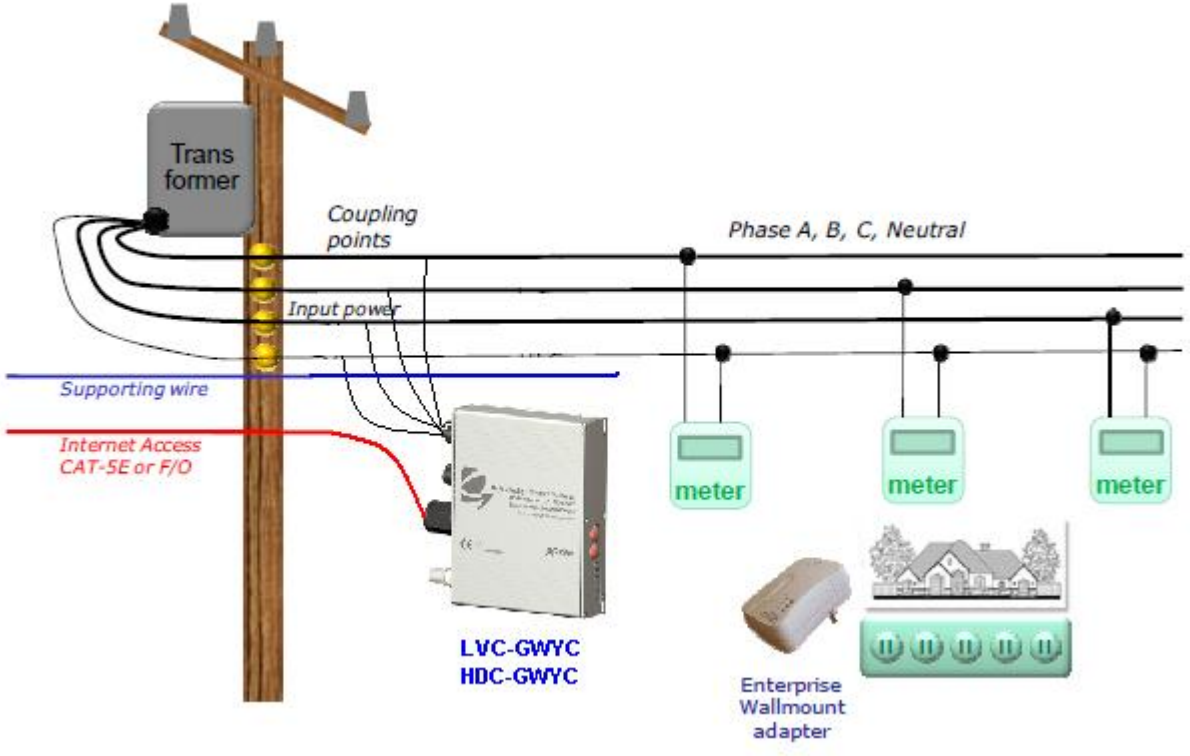


Figure 10: LV Gateway in a last-mile deployment

The second example shows an application in an MDU building where the Gateway is used to distribute the Internet access to multiple residential units using 3-phase 4-wire power system. Corinex 11+1 coupler is used for signal distribution together with inductive couplers to improve the signal strength on all 3 phase lines. Coaxial output is selected on the Gateway.

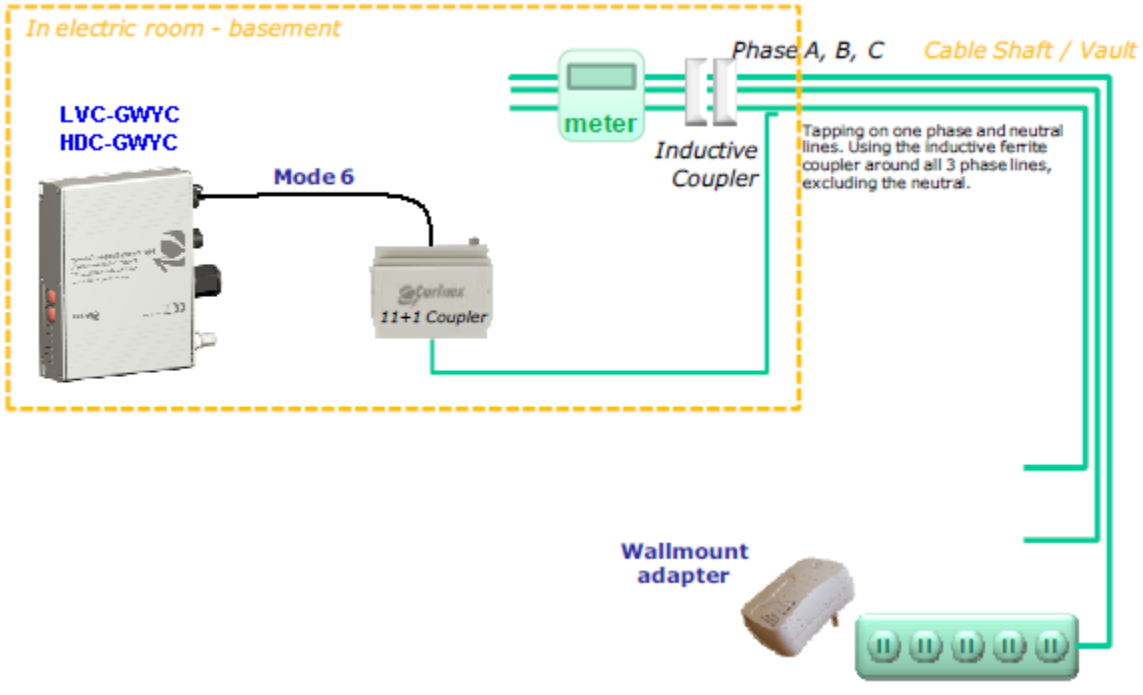


Figure 11: MDU application

The number of CPEs in the above example is limited to 31 according to the maximum number of BPL ports that each Gateway can provide. To extend the number of users, an HDC can be used for the HE Master unit with another LVC as a TDR unit. The HE unit connects to 14 CPE units and 1 TDR unit. The TDR unit connects to 31 CPE units. Total number of servicing users is 14+31 = 45. The maximum number of MAC addresses in this network is 1024+128 = 1152. A 2-way splitter used in this configuration will provide a separation between two Gateways enough to prevent from signal saturation. More TDR units can be deployed in order to increase the number of users. However, the network latency will be increased as the number of CPE units and activity of users' application.

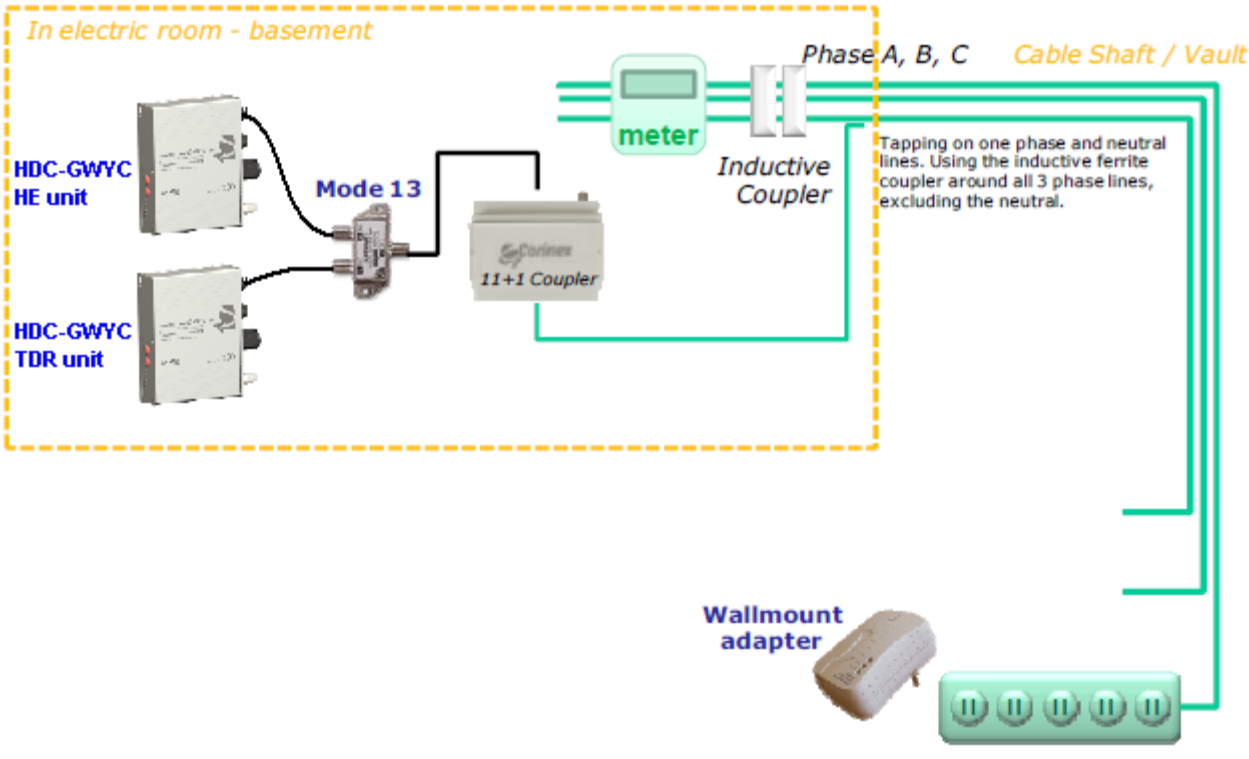

In electric room - basement
Phase A, B, C
Cable Shaft / Vault
meter
Inductive Coupler
Tapping on one phase and neutral lines. Using the inductive ferrite coupler around all 3 phase lines, excluding the neutral.
HDC-GWYC HE unit
Mode 13
11+1 Coupler
HDC-GWYC TDR unit
Wallmount adapter

Figure 12: High-density MDU application

TECHNICAL SPECIFICATIONS

Standards	ITU-T G.984.x, IEEE 802.3u, 802.1P 802.1Q, UPA Access Specification
Safety and EMI	EN 55022 Class B, EN 55024, EN 50412 EN 60950 - 1:2001 IEC 60950-1 :2001
Backbone speed	BPL: Up to 200 Mbps (PHY) Ethernet: 10/100 Mbps Full Duplex (AUTO)
Three phase coupler to power line	110VAC / 220VAC / 240VAC / 277VAC
Interfaces	Power line connector TNC-type female coaxial connector 10/100BaseT Fast Ethernet RJ-45 RS485 Serial Port
Powerline frequency range used	2 – 34 MHz
Power input	85 to 300 VAC, 50/60Hz
Dimensions	220 x 40 x 205 mm (including ports) 220 x 40 x 140 mm (not including ports)
Weight	2 Kg
Transmitted power spectral density	-50 dBm/Hz
Power consumption	Maximum 10 Watts
Operating temperature	-20° to 70°C (-4°F to 158°F)
Operating humidity	10% to 80% non-condensing
Environmental class	IP65

MAINTENANCE

- Unplug the cables including AC power, Ethernet, DC and Coaxial cable from the device if it is not used for an extended period of time, and put the caps on each of the connector.
- Store the device in a dry and cool place when not in use.
- Configuration settings saved in the NVRAM are kept permanently.

PROCEDURES OF PACKAGING, TRANSPORT AND STORAGE

❖ Packaging

Please see the diagrams below for packaging procedures.

1. Put the power cable into the box

2. Put the gateway and the mounting brackets into the box.

3. Make sure the serial number on the gateway matches the serial number on the box.

4. Put the top cover in the box, and then close the lid of the box.

❖ Storage

1. Storage environment: the ambient temperature shall be controlled at 15-30 ℃ and humidity must be controlled in 30 to 70%.

2. Electrostatic protection: the electronics is susceptible to electrostatic destructive effects, and it shall be properly stored against electrostatic damage.

ANNEX 1: CORINEX AV200 ENTERPRISE FEATURES

Introduction

This annex describes the features included in Corinex Enterprise firmware version 4.0.110 or as identified as ac_sv4_0_110_0_0_3_0_8 for AV200 product family.

Application Description

- **Core Features:** This section describes the core features, such as the protocols related to the PLC physical layer and the low level support for packet management;
- **MAC Layer:** Describes the components that compose the Medium Access Control layer;
- **Application Layer:** A description is given of the components that run above the core and MAC layers;
- **PLC Application:** This section describes some parameters specific to the PLC application;
- **Boot Process:** This section describes, by way of example, the start-up process.

Core Features

The core features are the protocols related to the PLC physical layer and the low-level support for the packet management.

802.1D Bridge Control

The bridge implements learning, ageing, forwarding, and the Spanning Tree Protocol (STP) as specified in 802.1D.

Bridge MAC Table Capacity

The bridge MAC table capacity is the number of different Ethernet MAC addresses that can be stored in the bridge in order to perform forwarding. Packets addressed to MACs not stored in the bridge table are replicated through all interfaces. In the current firmware implementation, the capacity of this table is varies by the model as follows:

Table 1: Maximum MACs in Bridge	
AV200 PRODUCTS	**MACs**
Low Voltage Compact Gateway	128
High Density Compact Gateway	1024

Learning Capacity

The learning speed is defined as the number of different MAC addresses per second received in the bridge and learned, with an unlearned ratio of less than 1% of the total MACs received. This value does not depend on the internal chip model.

Table 2: Learning Speed
750 MACs/second

Spanning Tree Protocol (STP)

The standard Spanning Tree Protocol is implemented in the current version, as described in the IEEE 802.1D standard (1998 edition). By default, the management VLAN is used to send the STP packets when VLANs are enabled.

Common Spanning Tree Protocol (CSTP)

The Common Spanning Tree (CSTP) protocol can be configured in the current version. With this variation of the STP, the STP packets are forwarded without a VLAN tag in the Ethernet/Gigabit Ethernet interfaces connecting the PLC network with the backbone.

Rapid Spanning Tree Protocol (RSTP)

The spanning tree protocol implemented includes the Rapid Spanning Tree, as described in the IEEE 802.1w standard. Rapid Spanning Tree Protocol (RSTP; IEEE 802.1w) is an amendment to 802.1D.

MSTP Frontier

The administrator should be able to define STP boundaries, so that bridge messages cannot pass through some pre-defined points. Therefore, topology changes would only be noticed within a limited region and hence convergence is faster. Only users directly affected by the link failure in the tree structure will detect a temporary (short) traffic cut during recovery.

Encryption Control

Corinex AV200 product family includes DES/3DES encryption feature. The current version of firmware has encryption disabled by default. However, it is possible to enable and configure it through the console. The supported key length is 56 bit by default. The use of 168 bits is available by special customized order.

Adaptive Bit Loading Control

The Adaptive Bit Loading Protocol is the software component responsible for adapting the modulation of each OFDM carrier, depending on the SNR of that carrier. This allows the highest possible throughput to be achieved with the current link quality. The main functionality of this component is:

- Change carrier modulation when the carrier SNR changes, adapting to the new link quality and avoiding line errors (if modulation is too high for the current link quality) or increasing efficiency (if the current link quality supports a better modulation);
- Carrier modulation does not follow linearly any SNR change, but must be filtered in time in order to reduce the probability of errors due to an unstable channel. Channel overload due to adaptive bit loading protocol packets must also be minimized. Therefore filters are included in both senses: not only to avoid any changes when they are not significant (i.e. slight improvement in only one carrier), but also with a smart algorithm that will learn from variations in SNR and modify the modulation accordingly;
- All ports are treated fairly, that is, their Bits Per Carrier (BPC) are evaluated with the same frequency. The period of BPC evaluation depends on the number of nodes visible in the network: the more nodes, the less frequent the measurements are, in order to avoid overload of the CPU;
- BPC measurements between a CPE and its master are interrupted when no data traffic is present, and therefore the CPE becomes idle;
- HURTO mode is the most robust transmission mode and is used when the channel condition is bad. Having connections in HURTO mode should be avoided in a network. No more than four connections

in HURTO mode (or with bits per symbol below 875) on the reception side should be allowed. Increasing that number may result in increased packet loss.

Service Classifier

The service classifier allows classifying the incoming packets from the input interfaces (Ethernet, FW and PL interfaces) to the power line. The computation of the priority is performed by means of a group of rules programmed by the firmware. There are two different criteria for computing the priority. The selection of the criteria is based on the match of a determined field of the Ethernet frame with one predefined pattern. Once a criterion is chosen, the priority is computed according to the parameters in that criterion. This method of prioritization allows for computing the priority of different packets using different fields and bit patterns. For example, there can be a difference in the computation of the priority depending on whether the packet is an IP packet or not. If the packet is an IP packet, then the priorities assigned can match those of the TOS field. Service classifier configuration can be specified in the auto-configuration file.

VLAN/OVLAN

802.1Q VLAN Support

Corinex AV200 product supports the use of Virtual LAN (VLAN), specified in the IEEE 802.1Q standard. It also keeps track of the priority field described in the 802.1p standard. The service classifier can use this field to prioritize traffic.

The basic VLAN configuration is service guided. Different VLANs are configured in the PLC network according to the type of data:

- Reserved VLAN (used for PLC protocols);
- Management VLAN;
- Data VLANs;
- VoIP VLANs.

Each of these VLANs can be configured with a different priority. The reserved VLANs are fixed to VLAN 1 and VLAN 4094. VLAN 0 is not supported.

Custom VLAN

Corinex AV200 product allows enabling the custom VLAN/OVLAN. When you enable this feature, you can completely configure the different ports in VLAN terms.

With a custom VLAN you can:

- Enable VLAN tagging in Ethernet ports;
- Change the VLAN port filtering behavior:
    - Forbidden lists: Packets with tags in the list are dropped;
    - Allowed lists: Packets with tags different from the ones in the list are dropped;
- Change the VLAN port filtering tag lists;
- Enable/disable the Out Format of the ports:
    - Enabled: Packets transmitted with a VLAN tag;
    - Disabled: Packets transmitted without a VLAN tag;
- Enable/disable the Tagged Only of the ports:
    - Enabled: Input untagged packets are dropped;

    - Disabled: All input packets are accepted;
- Enable/disable the ingress filtering (egress filtering is always performed when the VLAN is active).

VLAN Tag Translation

Corinex AV200 product allows tag translation in Ethernet interfaces. Packets coming with tag A from the Ethernet interface are retagged with tag B inside the PLC network. When a packet with tag B exits the PLC network in the same interface, it is retagged to the A source tag. Only one tag translation can be used per Ethernet port.

OVLAN

Corinex AV200 product supports OVLAN, a mechanism independent from the VLAN. OVLAN tagging is similar to VLAN tagging, but it is only used inside the PLC network. The OVLAN tags are not propagated outside the PLC network.

The basic OVLAN configuration uses only one OVLAN tag (ROOTPATH) to allow the isolation of all end users of an access network. Another OVLAN tag (0) is reserved for PLC protocols.

Custom OVLAN

Corinex AV200 product allows enabling the custom VLAN/OVLAN. When you enable this feature, you can totally configure the different ports in OVLAN terms, similar to VLANs.

With a custom OVLAN you can:

- Enable OVLAN tagging in Ethernet ports;
- Change the OVLAN port filtering behavior:
    - Forbidden lists: Packets with tags in the list are dropped;
    - Allowed lists: Packets with tags different from the ones in the list are dropped;
- Change the OVLAN port filtering tag lists;
- Enable/disable the Out Format of the ports:
    - Enabled: Packets transmitted with a VLAN tag;
    - Disabled: Packets transmitted without a VLAN tag;
- Enable/disable the Tagged Only of the ports (only PLC ports):
    - Enabled: Input untagged packets are dropped;
    - Disabled: All input packets are accepted;
- Enable/disable the Accept Tagged of the ports (only Ethernet ports). This is useful in implementing frequency division repeaters:
    - Enabled: Input tagged packets are accepted;
    - Disabled: Input tagged packets are not accepted.
- Enable/disable the ingress filtering (egress filtering is always performed when the VLAN is active).

VLAN/OVLAN Limitations

The number of supported VLANs depends on the modem's configuration. The hardware has an internal table, in which the VLAN information is stored. This table is unique and is shared by all interfaces in the modem. The elements in this table can be linked to create lists. This table is used to store the VLAN and OVLAN configuration (list of tags).

The configuration for each interface is a pointer to an entry in this table. The list of tags can be configured as allowed or forbidden tags. The 'forbidden tags' can be used to allow all of the possible VLAN tags except a

reduced list of tags that are not allowed (forbidden).

With the current implementation of the FW, it is not possible to share lists of tags between different interfaces. The total number of tags that can be used is limited by the following equation:

$$\sum_{port=0}^{MAX\_PORTS}(VLAN + OVLAN) + \sum_{ETH\_A}(VLAN + OVLAN) + \sum_{ETH\_B}(VLAN + OVLAN) + \sum_{FW}(VLAN + OVLAN) \leq Max\_Num\_Tags$$

There is also a limitation per port, as detailed in Table 3.

Table 3: Maximum VLAN Tags

MODEL in AV200 PRODUCT LINE	TOTAL VLAN TAGS
LV & HD Compact Gateway	16

MAC Filtering

MAC filtering allows limiting access to the PLC network through the Ethernet interface to a certain number of source MAC addresses. The maximum number of allowed addresses is 4. There are two working modes:

1. **FIXED mode:** The allowed MAC addresses are specified in the auto-configuration file;
2. **AUTO mode:** The allowed MAC addresses are the first ones learned by the Ethernet interface until the maximum number of allowed MAC addresses is reached.

Spatial Reuse

This feature tries to maximize the efficiency of the simultaneous use of the physical channel. The spatial reuse relies on two basic tools to do its work, the Power Control and the Sub-modes.

Power Control

This feature only affects slaves. When enabled, the slaves will try to reduce their transmission gain maintaining the BPC value of their link with the master node over a certain threshold.

Sub-modes

The sub-modes are modes that share the same spectrum but are not mutually compatible. In this way one modem in a sub-mode sees a modem in another sub-mode as white noise and they do not disturb each other.

Power Mask Control

The Power Mask (PM) is a transmitted Power Spectral Density (PSD) frequency mask that is used to prevent or decrement transmitted Power in some bands giving a particular “shape” to the PSD. There are three different PM concepts; the Mode PM (MPM), the Regulation PM (RPM) and the Raw PM (RawPM).

- **Mode Power Mask**: The MPM is associated to a transmission mode (tx mode) definition, this power mask is always merged with types of power mask if they are configured, so it is the only one set in the Hardware if RPM and RawPM are disabled;
- **Regulation Power Mask**: The RPM is transmission mode independent and it is defined by a set of attenuated bands called notches, each of which are defined by its start frequency, stop frequency

and depth where the frequencies are specified in KHz and the depth in dB. The carriers in a notch are removed from the output signal, and the depth is used to calculate the slope of the PSD frequency mask, so its value affects the carriers adjacent to the notch. The objective of the RPM is to comply with PSD regulations that prohibit interference in certain bands such as those used for amateur radio, and to guarantee that the PSD inside the notch has a level at least "deep" dB under the maximum level of the PSD outside it;

- **Raw Power Mask**: The RawPM is the carrier defined mask downloaded in the auto-configuration file and preceded by the identifier GENERAL_SIGNAL_POWER_MASK. It is always applied when the download is correct and is transmission mode independent, so particular carriers are attenuated. Care should be taken when there are additional transmission modes as these can be removed. RawPM is only recommended when a modem uses one transmission mode.

The three types of PM are always merged to obtain the most restrictive PSD, which means the minimum transmitted PSD for each carrier or, in other words, the maximum value for PM for each carrier. So, MPM is always applied and may be different for each tx mode. If RPM is enabled, its carrier coefficients are calculated for each tx mode and merged with MPM. RawPM is merged with the MPM and the RPM (if enabled).

NOTE: Certain limitations must be taken into account when defining new Power Masks:

- There must be a minimum of 20 non-attenuated carriers between notches;
- At least one quarter of the band must be unmasked.

It must be taken into account that these limitations should be used as a reference and not as an exact value.

MAC Layer

LV Access MAC & QoS

Bandwidth Limitation

Bandwidth limitation is a feature that limits the amount of data a node can transmit and receive. It does not provide any guarantees on the obtained throughput, although, where possible, the targeted limit will be achieved within some margin of error.

For low bandwidth limits, the bandwidth obtained after limitation is not accurate. However, it is possible to predict the value that will be obtained by using the following graph. Anyway the final value and the marginal error will depend on the physical level, the protocol efficiency, the latency step configured and the number among other factors.

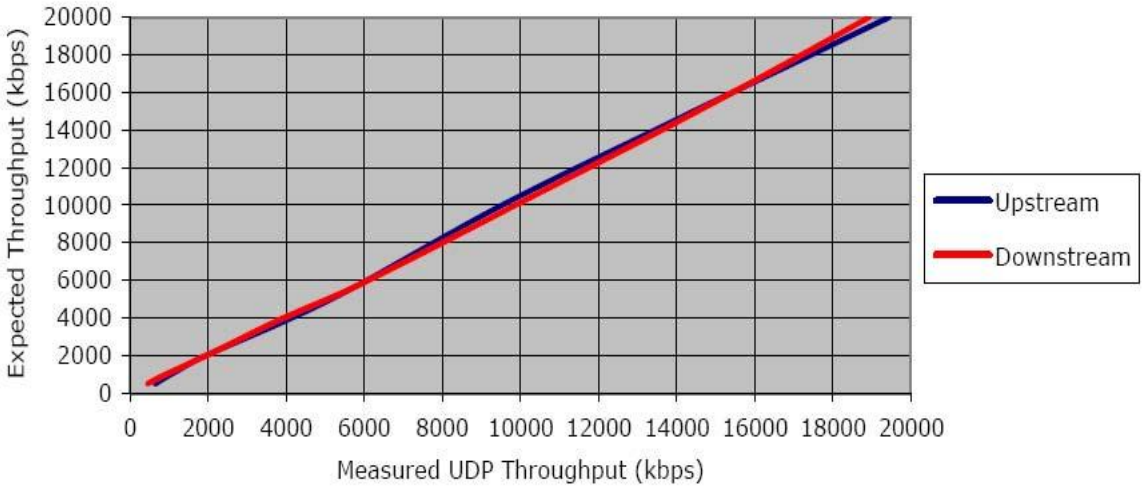


Figure 17: Expected Throughput vs. Measured Throughput

This graph has been obtained considering a HE-CPE scenario with good physical level and the entire default configuration, except for the bandwidth limitation that is configured in each case with a different test value. The traffic sent is a unidirectional UDP flow (upstream or downstream) with a higher rate (at least double) than the bandwidth limitation configured.

The characteristics of the algorithm are shown in Table 4.

Table 4: Bandwidth Limitation
PARAMETER VALUE
Minimum Speed 512 Kbps
Maximum Speed 20000 kbps
Convergence Time 30 sec
Speed Fluctuation <10%

Latency management

The latency management is achieved through a set of features, designed to guarantee Quality of Service. The Service Classifier can be configured to prioritize the traffic according to the desired criterion (TOS, VLAN tag or any other configured) and each of the PLC priorities (from 0 to 7) assigned by the Service Classifier has a Service Level Agreement (SLA1, SLA2, SLA4 and SLA8) associated.

CSMA/CARP MAC

The CSMA/CARP MAC is implemented in the current firmware version. The CSMA/CARP MAC can be activated by selecting GENERAL_MAC_MODE = INHOME in the auto-configuration file.

Layer 2 ACKs

It is possible to configure layer 2 ACKs according to the priority of the traffic being transmitted. The ACK policy is unique per connection, and must be the same per packet: if several priorities are sniffed the policy will be fixed by the maximum SLA detected. Layer 2 ACKs are enabled by default in every power line connection, for all data priorities.

Application Layer

TCP/IP Stack

The firmware includes a TCP/IPv4 stack supporting the IP, UDP, TCP, ARP and ICMP protocols. The stack itself is not needed for the basic PLC modem functionalities, but it helps in remote accessibility, mainly for configuration purposes. The UDP/TCP protocols allow creating sockets with other IP machines and using high-level protocols such as FTP, HTTP, etc. As a limitation, this TCP/IP stack does not support IP fragmentation. The maximum packet size allowed is 1514 bytes.

TFTP Client

The firmware includes a Trivial File Transfer Protocol (TFTP) client that allows downloading files from a TFTP server. This is the simplest way to transmit files. It is primarily used for downloading new firmware versions, and downloading auto-configuration files. The drawback of this protocol is that has no error correction and uses UDP.

The maximum downloaded file size is listed in Table 5.

Table 5: Maximum Downloaded File Size

OPERATION	SIZE (KB)
Configuration file	50
Other file downloaded using a console command	26.5

The file name can be up to 256 characters long.

FTP Client

The firmware includes a File Transfer Protocol (FTP) client that allows downloading or uploading files from an FTP server. This is a more robust protocol for downloading files. The FTP protocol uses a TCP connection and is able to confirm whether or not the file has been correctly downloaded or uploaded. It is used primarily for downloading new firmware versions, and downloading and uploading auto-configuration files. The limitations regarding file size and name length are the same as in the TFTP client.

DHCP Client

The modem includes a DHCP client to automatically configure the basic IP parameters (IP Address, Subnet Mask and Default Gateway address). The system supports the DHCP extensions and configuration file downloading.

Link Search

The Link Search protocol is the first protocol that takes place when a CPE is started. Its aim is to select a link (or transmission mode) amongst a list of links in which an access network is detected. Each link is tested for Tseconds. The CPE will select the first link in the list and will configure the transmission mode. After T_{link} seconds, if no access network is detected, the transmission mode will be changed to the next one in the list. The worst-case time to detect an access network if Nis the number of links in the list is:

$$N_{links} \times T_{link} \times N_{submodes}$$

The default values are:

T_{links} 5 seconds

N_{links} 13 links
$N_{submodes}$ 4 submodes

Access Protocol/Roaming

When a CPE detects an access network, it will start the Access Protocol in order to obtain access to the network. The master and the TD repeaters present in the network send continuous invitation or access tokens. The CPE will select the best master according to certain criteria, and will answer this invitation token in order to access the network through this master. The master might deny access to the CPE, in which case the CPE will select a different master and will try to access the network through that master.

If access to the network is not allowed through any visible master in the network, the CPE will restart the link search protocol, in order to find a new link.

Once a CPE is connected to a master, it can re-evaluate its status periodically, and can change its connection to a new master, according to certain criteria. This phase is known as the second step.

The default configuration has been chosen in order to avoid instabilities: its frequency is very low, and the change of master will only occur if the current master has very bad SNR.

- The second step takes place after the auto-configuration process and every three hours.
- The SNR threshold required to change masters is the equivalent to 2,150 bps (nonfiltered reception value).

Auto-configuration

The objective of the auto-configuration process is the centralized management of a BPL network using configuration files stored in a centralized database that are transferred to each piece of equipment when it boots. These files contain all of the information that a node needs in order to function in a correct manner.

Below is a brief description of the process which is discussed in more detail later in the manual:

1. Every node starts with the same default factory configuration: Access CPE;
2. Using PTTP (Parametric Translation Table Protocol) the modem discovers if it is booting in a network with VLANs or not. If a network has been built using VLANs to isolate traffic between data, voice over IP or management traffic, it is necessary to know the Management VLAN of that network segment for the DHCP request to reach the backbone. The information passed between modems during PTTP is called the translation table;
3. Using DHCP protocol, each node gets its IP configuration (IP address, netmask and gateway) and the name of its corresponding auto-configuration file;
4. Using TFTP protocol, the nodes download the auto-configuration file and configure the firmware accordingly.

In addition to the main steps outlined above, but there is further point to consider:

In order to achieve a secure network, powerline (PL) authentication is introduced. When a new slave is trying to access the PL network and connecting to a master or a repeater, the master or repeater may perform a RADIUS request to authenticate the user. The RADIUS server will reply with information used to configure the master's interface to the new user. However, auto-configuration also has a way to avoid using the RADIUS server if desired. This consists of declaring a list of MACs, profiles and FW type in the auto-configuration file and using this list instead of RADIUS to

authenticate the users.

If the node is the first modem in the network and connected directly through the Ethernet port to the backbone, the auto-configuration process is different:

1. This node starts with the same default factory configuration: Access CPE;
2. Using DHCP protocol, each node gets its IP configuration (IP address, netmask and gateway) and the name of its corresponding auto-configuration file. There is also another parameter called PTTP-code that indicates if VLAN is used and the value of the management VLAN if needed. Once this parameter is obtained the PTTP protocol finishes;
3. Using TFTP protocol, the nodes download the auto-configuration file and configure the firmware accordingly.

When any node boots, there is a parameter stored in the NVRAM called GENERAL_USE_ AUTOCONF. When this value is 'yes', the node boots in auto-configuration mode and when 'no', it boots in NVRAM mode. There are two auto-configuration possibilities inside the auto-configuration boot mode depending on whether or not PTTP is performed.

Auto-configuration-PTTP Boot

In this auto-configuration boot modality, the node always initiates as a slave (CPE) and starts to send PTTP requests. When this protocol ends, the modem has the minimum information to successfully connect to the backbone and execute DHCP and TFTP. The node then performs a DHCP request to get an IP configuration, and the name of the auto-configuration file (option 18), as well as the TFTP server where the file is located (option 66). It then downloads the file and configures the firmware accordingly.

Auto-configuration-no PTTP Boot (default)

In this auto-configuration boot modality, the modem has been already configured to successfully execute DHCP and TFTP so it skips PTTP.

NVRAM Boot

When a node starts in NVRAM mode, it collects all of the configured parameters from the NVRAM memory and configures the firmware accordingly. There are some basic parameters that are always configured in this mode:

- GENERAL_TYPE: Node type = HE, CPE, or TDREPEATER.
- GENERAL_IP_USE_DHCP: Use DHCP = YES or NO. If this parameter is set to NO, the IP configuration parameters are configured from NVRAM.

All the other parameters are only configured if they have been downloaded from a file first, and a GENERAL_USE_AUTOCONF = NO line was in that auto-configuration file. This is equivalent to performing a Save as Permanent.

PTTP Protocol

The PTTP (Parametric Translation Table Protocol) is used to transfer the translation table between modems at booting. The translation table is comprised mainly of VLAN and OVLAN parameters. When a modem boots using auto-configuration mode with the current firmware version, it skips PTTP requests and doesn't run PTTP client unless it is set by Telnet CLI command. The Telnet CLI command to enable PTTP client is ">ac

pttpmode set 1". This command will write a byte in NVRAM in order that the next boot mode of the modem will start with PTTP client.

PTTP Booting

When a modem boots in auto-configuration mode, it starts sending PTTP requests. The modem needs to know if it is booting in a network with VLANs before requesting an IP through DHCP. For this reason, and because the LV node does not know if communication to the MV node is through PLC or Ethernet, the FW-to-FW protocol uses a special PTTP MAC (01:80:C2:00:00:0E) if communication is via Ethernet the LV node does not know the MAC of the MV node. The PTTP petitions are performed in the following steps:

Step 1: A PTTP request is made without VLANs and waits for a response;
Step 2: It then switches to VLAN mode and makes a PTTP request using tag #1 (reserved in the BPL network) and waits for a response;
Step 3: Returns to Step1.

When a node receives a packet with this PTTP MAC, the packet is sent to the FW. In transmission, this request is forwarded to all active interfaces. Finally it will connect to a node that will transfer the translation table. The modem switches automatically to use or not to use VLANs with the same configuration as the node sending the translation table. In this way all modems configure themselves to use or not to use VLANs. This avoids having to write the use or non-use of VLANs in the NVRAM of all modems, a circumstance that can be extremely convenient if an operator wants to change the entire network to use VLANs.

A modem must not perform PTTP (in Auto-configuration-no PTTP Boot mode) in the NVRAM in the following two cases:

- If it is the first node of the network (directly connected to the backbone);
- If it is going to receive the translation table in the auto-configuration file.

In the first instance, this node will transfer the translation table (included in the auto-configuration file) to other modems when requested, but in this case there is no other modem from which to request this information because it will be the first node to know it.

To avoid using PTTP in the boot process, two methods are available:

1. Using the DHCP server (must be accessible through VLAN #1 or without VLAN), the PTTP protocol can be skipped. In the DHCP reply, the server can supply the modem with the management VLAN (in the event the modem boots in VLAN mode) or tell the modem not to use VLANs;
2. Write a byte in the NVRAM using console. In this type of boot the modem reads its NVRAM to check if it has to use or not to use VLANs and the Management VLAN (if needed), requests an IP from the DHCP server and finally receives its auto-configuration file via TFTP.

The second method is not advisable, because the access to the console is poor while using PTTP due to the change between VLAN and no-VLAN modes. Method 1 should therefore be used if possible.

To disable PTTP through DHCP (method 1), see the detail about DHCP client.

If no OVLANs or VLANs are going to be used in the network, the PTTP protocol can be disabled in all of the modems. To disable PTTP manually in the next boot of a modem, follow the steps below:

- Using a DHCP server, give an IP to the modem; this may take some time because, sometimes, the modem will be sending DHCP requests with VLAN #1 and others without VLAN active;

- Once the modem has an IP, log in to the console and execute the commands below (NOTE: Due to VLAN switching, the console may seem to hang; if this occurs, log out from the console and log in again):
    - ac stop: Stops the auto-configuration process (and also PTTP) and disables the VLANs. It is advisable to execute this command first to work comfortably with the modem. This command does not write anything in the NVRAM, so it only takes effect when the modem is reset;
    - ac pttpmode set 0: Disables PTTP in the next boot, writing in the NVRAM. ("ac pttpmode set 1" enables PTTP in the next boot, writing in the NVRAM);
    - ac pttpmode get: Checks the PTTP state for the next boot, reading the NVRAM.

NOTE: DHCP should be used (if possible) to disable PTTP.

SNMP Agent

This release supports SNMP v1, without support to variable bindings for traps, and with a single community name. The following MIBs are supported.

Table 6: MIB Tables	
CORINEX MIB	
MIB II	RFC 1213
CORINEX ACCESS MIB	

The available OIDs included in MIB II have been extended to all interfaces in the modem. The default community names for SNMP read and write are set to 'public' and can be changed by Telnet CLI command in admin mode.

FLASH Upgrade Protocol

The FLASH upgrade protocol allows provision for an upgrade of any of the binaries included in the firmware release. A secure upgrade of the application and the loader binaries is ensured by the existence of a backup image. This however does not provide any protection from the download with a non-running or incorrect application or loader.

BIST The Built-In Self Test (BIST) provided in this release executes by default the following tests:

- **Memories:** The loader checks the data and address buses of the DRAM, as well as the CRC of every FLASH section;
- **Ethernet:** The Ethernet PHYs are set in loopback mode in order to test communication. (disabled by default to reduce boot time);

RADIUS Client

The RADIUS client is compliant with RFC2865, except for the accounting functionalities that are not included.

Multicast There are two possible options to configure multicast features:

IGMP PacketDetection (IGMP Aware Multicast Syndication)

If IGMP packet detection feature is enabled, the end point parses all upstream packets looking for IGMP "join" and IGMP "leave" datagrams. All upstream traffic must be "sniffed" by the internal processor by

passing these packets up to firmware and checking whether they contain IGMP control messages. When an IGMP control message is detected, the end point sends control messages to all PLC network elements in the transmission chain (end point and access point) to reconfigure all bridges to ensure that they are syndicated to the new multicast stream and no traffic replication is made. This feature can be dynamically enabled or disabled.

External Multicast Configuration (MPP)

It is possible to configure multicast by sending "special" frames to the modems, communicating the creation of new bindings and the deletion of old ones. Encapsulation is the general method to exchange data between PLC nodes using the LLC layer. Customers can determine what information is exchanged, build and send their own messages, and allow actions to be taken when these messages are received, if necessary. With this method, the external devices (not PLC) "translate" the IGMP join/leave frames to MPP frames relayed to the modems which configure the multicast bindings.

Factory Reset

Users can restore the modem to a default state if any problem occurs by the factory reset command in Telnet CLI session.

PLC Application Description

The PLC application specification is described in the following subsections.

Modes Definition

The parameters that define a mode are as follows:

- **Central Frequency:** Indicates where the mode is placed in the spectrum (in Hertz);
- **Bandwidth:** This is the real bandwidth of the mode. It depends on the mode bandwidth and power mask used;
- **Mode Bandwidth:** It can be 10, 20 or 30 MHz defines the maximum usable bandwidth in the mode;
- **PSD at the DAC Output (theoretical):** Depends on the configuration of the internal digital amplifiers/attenuators. The real value can be slightly different depending on the external AFE and their configuration. The value provided is the theoretical configured by firmware. The device characterization has demonstrated that the measured PSD is very close to this theoretical value and also can be checked with PSD at the line after AFE gain. The final power on the line depends on the gain of the AFE;
- **Power Mask Definition:** This is the power mask definition used in this mode;
- **Maximum Physical Speed (achievable in this mode):** The maximum bps depends on the bandwidth mode, the power mask, and some other secondary parameters, such as BPC thresholds, configuration for BER, maximum allowed SNR in the RD, etc. The value provided is the theoretical value for the default modem configuration and includes all overhead introduced in the physical layer.

Mode 1

Table 7: Mode 1	
PARAMETER	**VALUE**
Central Frequency	7.968.750 Hz
Bandwidth	10 MHz
Mode Bandwidth	10 MHz
PSD	-72 dBm/Hz
Power Mask Definition	Flat PM
Maximum Physical Speed	84 Mbps

Mode 2 (A1 MVG)

Table 8: Mode 2	
PARAMETER	**VALUE**
Central Frequency	18.437.500 Hz
Bandwidth	10 MHz
Mode Bandwidth	10 MHz
PSD	-72 dBm/Hz
Power Mask Definition	Flat PM
Maximum Physical Speed	84 Mbps

Mode 3 (A1 MVG)

Table 9: Mode 3	
PARAMETER	**VALUE**
Central Frequency	29.062.500 Hz
Bandwidth	10 MHz
Mode Bandwidth	10 MHz
PSD	-72 dBm/Hz
Power Mask Definition	Flat PM
Maximum Physical Speed	84Mbps

Mode 6

Table 10: Mode 6	
PARAMETER	**VALUE**
Central Frequency	19.062.500 Hz
Bandwidth	30 MHz
Mode Bandwidth	30 MHz
PSD	-77 dBm/Hz
Power Mask Definition	Flat PM
Maximum Physical Speed	205 Mbps

Mode 7

Table 11: Mode 7	
PARAMETER	**VALUE**
Central Frequency	7.031.250 Hz
Bandwidth	5 MHz
Mode Bandwidth	10 MHz
PSD	-72 dBm/Hz
Power Mask Definition	Lower Half Band
Maximum Physical Speed	42 Mbps

Mode 8

Table 12: Mode 8	
PARAMETER	**VALUE**
Central Frequency	12.812.500 Hz
Bandwidth	5 MHz
Mode Bandwidth	10 MHz
PSD	-72 dBm/Hz
Power Mask Definition	Lower Half Band
Maximum Physical Speed	42 Mbps

Mode 10

Table 13: Mode 10	
PARAMETER	**VALUE**
Central Frequency	7.031.250 Hz
Bandwidth	10 MHz
Mode Bandwidth	10 MHz
PSD	-72 dBm/Hz
Power Mask Definition	Flat PM
Maximum Physical Speed	84 Mbps

Mode 13

Table 14: Mode 13	
PARAMETER	**VALUE**
Central Frequency	17.031.250 Hz
Bandwidth	30 MHz
Mode Bandwidth	30 MHz
PSD	-77 dBm/Hz
Power Mask Definition	Flat PM
Maximum Physical Speed	231 Mbps

Mode 2 (for A2 MV Gateway)

Table 15: Mode 2 – A2	
PARAMETER	**VALUE**
Central Frequency	17.500.000 Hz
Bandwidth	7 MHz
Mode Bandwidth	10 MHz
PSD	-72 dBm/Hz
Power Mask Definition	M11 PM
Maximum Physical Speed	60 Mbps

Mode 3 (for A2 MV Gateway)

Table 16: Mode 3 – A2	
PARAMETER	**VALUE**
Central Frequency	27.031.250 Hz
Bandwidth	10 MHz
Mode Bandwidth	10 MHz
PSD	-72 dBm/Hz
Power Mask Definition	Flat PM
Maximum Physical Speed	84 Mbps

Power Mask and Notches

A dynamically configurable power mask allows the possibility to have fully configurable notches in the desired frequencies. By default, the power mask configured will depend on the mode used as described above. A different power mask can be configured through the auto-configuration process.

The Power Mask can be defined as part of the modem definition, as a regulation Power Mask, defining the frequency bands and the attenuation, or a raw Power Mask applied directly to every carrier.

The following default Power Mask definitions are included, and used in some modes.

Flat PM

No carrier is attenuated.

Upper Half Band PM

This Power Mask uses the Upper half carriers. The lower half carriers are completely attenuated.

Lower Half Band PM

This Power Mask uses the lower half carriers. The upper half carriers are completely attenuated. M11 PM

This Power Mask uses all carriers except the first 96 and the last 149 carriers, which are completely attenuated. It is used for Mode 11.

OLD M11 PM

This is similar (but slightly different) to the previous one. It is used for backward compatibility.

IARU PM

The IARU power mask is defined as the default value of the regulation Power Mask. IARU PM is composed of 19 notches in Corinex products. The settings are listed in Tables below.

Table 17: IARU Power Mask Description

NOTCH NUMBER	STARTING FREQ – ENDING FREQ	NOTCHING (ATTENUATION/BW)
0	1800-2000	>30
1	2850-3025	>30
2	3400-4000	>30
3	4650-4700	>30
4	5330-5405	>30
5	5450-5680	>30
6	6525-6685	>30
7	7000-7300	>30
8	8815-8965	>30
9	10005-10150	>30
10	11275-11400	>30
11	13260-13360	>30
12	14000-14350	>30
13	17900-17970	>30

Table 18: IARU Power Mask Description

NOTCH NUMBER	STARTING FREQ – ENDING FREQ	NOTCHING (ATTENUATION/BW)
14	18068-18168	>30
15	21000-21450	>30
16	21924-22000	>30
17	24890-24990	>30
18	28000-29700	>30

The purpose of the power mask is to avoid an injection of signal that may disturb other technologies. The IARU power mask can be applied by enabling the regulation Power Mask without changing its initial definition. It will be applied to all relevant transmission modes. It is configurable through Telnet CLI, auto-configuration, and SNMP interface.

PLC Ports

The PLC ports are used as an index to refer to a modem that is visible through the power line. Therefore

ports are not only used for the master and its slaves, but also for any other visible modem. When the limit of the number of ports is established as N_{max_ports}, this means that a modem can see up to N_{max_ports} modems, all of which are not necessarily its slaves. The order in which the ports are associated to modems is "first come first serve". Also, every multicast MAC address uses one entry in this table. There is an additional broadcast port to those regular ports. The number of ports depends on the chip model used in Corinex products. The following table shows the values for the current release.

Table 19: Maximum PLC Ports	
Corinex product model	Ports
Low Voltage Compact Gateway	31
High Density Compact Gateway	15

Boot Process

The start-up process of the modems is described, step-by-step, using the scenario shown in Figure 18 – one PC connected to a modem (modem 1, which will be the master) through the Ethernet. A second modem (modem 2, CPE) is connected to the first modem through the power line.

The PC contains all of the necessary servers: DHCP, TFTP, RADIUS, etc. The steps are going to be described conceptually, so a detailed configuration of the server is not going to be provided.
The following tables describe the steps followed by the two modems; each row represents some amount of elapsed time although this elapsed time can be different from row to row. To indicate coincidences of time in the two modems, the cells in the tables are marked with a (number). The tables are divided into two columns, one representing the application tasks and the other the PLC layer.

Both modems are powered on. The boot process described above is completed, the OS is running and the tasks are started.

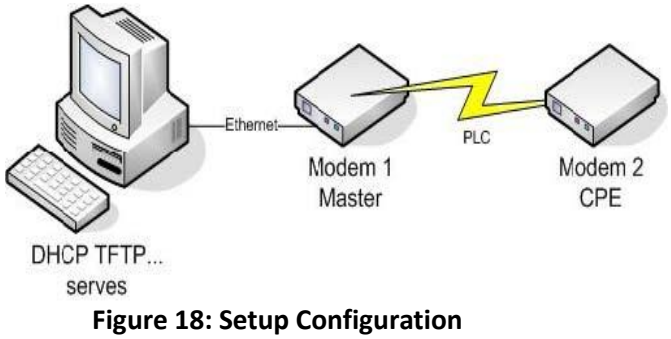


Figure 18: Setup Configuration

Modem 1:

Table 20: Master Boot Description (Modem 1)	
APPLICATIONS PLC	
If STP is enabled, the ports must be in the forwarding state before any packet can be sent through the port. The STP task sends STP packets through all ports (PLC if exists and Ethernet) to detect loops.	Modem starts as a slave.
The DHCP task sends DHCP request through all ports (PLC if exists and Ethernet) asking for IP address.	Link Search starts looking for synchronization.
The PTTP task sends PTTP queries through all ports (PLC if exists and Ethernet).	Although there is no master, Modem 1 is continuously changing the link trying to synchronize.

If PTTP is enabled, DHCP messages are sent with VLAN (802.1Q) tag 1 and without a VLAN tag alternatively.	
The DHCP server of the PC responds with the IP, PTTP parameter, IP of the TFTP server, and configuration file name.	
The DHCP task responds with DHCPACK to the server, stops sending DHCP request packets and passes the parameters to the PTTP task (PTTP parameter) and to the autoconfiguration task (TFTP server IP and configuration file name).	
The PTTP task stops sending packets.	
The PTTP task acts according to the PTTP parameter, gets the DHCP, thus VLAN configuration is set.	
The modem is now accessible through TCP/IP, so tasks like the console and SNMP are awaiting any input to respond.	
The Autoconfiguration task downloads the configuration file using TFTP.	
The Autoconfiguration task uses the parameters to configure the modem.	
	The modem changes to master.
	The link is changed to that of the autoconfiguration.
Autoconfiguration ends.	The master starts sending access tokens, so slaves can request access.
……	……
	One slave is detected.
The RADIUS task sends a RADIUS query for the MAC of the slave.	Port solver protocol starts negotiating the ports.
The RADIUS task receives the authorization of the RADIUS server with the desired profile for the user.	
	Port solver protocol (PSP) ends the port negotiation.
QoS and network parameters are configured for the new user: bandwidth limitation in upstream and downstream, VLANs, OVLANs, etc.	The token is shared between the master and the slave, so the slave can send data packets.
The PTTP task receives a request from the slave.	
The PTTP task sends an answer to the slave with the translation table and the management VLAN.	

Modem 2:

Table 21: CPE Boot Description (Modem 2)	
APPLICATIONS PLC	
If STP is enabled, the ports must be in the forwarding state before any packet can be sent through the port. The STP task sends STP packets through all ports (PLC if exists and Ethernet) to detect loops.	Modem starts as a slave.
The DHCP task sends DHCP request through all ports (PLC if exists and Ethernet) asking for IP.	Link Search starts looking for synchronization.
The PTTP task sends PTTP queries through all ports (PLC if exists and Ethernet).	Synchronization is achieved in one of the links.

If PTTP is enabled, the DHCP messages are sent with VLAN (802.1Q) tag 1 and without a VLAN tag alternatively.	Access protocol detects a master.
	Access protocol answers access token of the master.
	Port solver protocol starts negotiating ports.
	Master grants the slave access.
	Port solver protocol ends the port negotiation.
The STP task sets the port in forwarding, so packets can go through PLC.	
The PTTP task receives the translation table and the management VLAN from the master.	
The PTTP task stops sending packets.	
Network parameters are configured in the ports according to the PTTP information.	
The DHCP server of the PC responds with the IP, IP of the TFTP server and configuration file name.	
The DHCP task responds with DHCPACK to the server, stops sending DHCP request packets and passes the parameters to the autoconfiguration task (TFTP server IP and configuration file name).	
The modem is now accessible through TCP/IP, so tasks like the console and SNMP are awaiting any input to respond.	
The Autoconfiguration task downloads the configuration file using TFTP.	
The Autoconfiguration task uses the parameters to configure the modem.	
Autoconfiguration ends.	

These operations result in an approximate time between reset and ping of (for a single pair of modem):

Modem 1: 40 seconds
Modem 2: 140 seconds

Constraints for Network Design

Two Master Visibility

Visibility between masters at physical level must be avoided. It is recommended to use spatial reuse procedures to avoid the direct visibility between HEs in the same mode (power control and sub-mode).

Maximum Allowed PLC Ports

The capacity of PLC ports is 32 in most of the products including MV Gateway, MDU Gateway, LV and GPON-BPL Gateway basic model, Powerline Adapter, and CableLAN Adapter. The High-Density LV and GPON-BPL Gateway have a capacity of 64, the Low Voltage Compact Gateways has capacity of 31 and High Density Compact Gateways have a capacity of 15.

Bridge Table Capacity

The maximum number of MAC address in the bridge table depends on the learning speed, the ageing time, and the packet switch capacity. The data provided is measured with the default configuration. To obtain the

maximum capacity in the bridge table, increasing the ageing time is recommended.

Bandwidth Limitation

The real bandwidth differs slightly from the specified limit and depends on a number of factors, like traffic type, number of users, channel conditions, line conditions, etc.

Reconfiguration Time in MV MAC

The protocols and algorithms that allow the reconfiguration of ring topologies in a short time (a few seconds) when a problem in the network appears are not included.

Regulation Power Mask

The regulation calculated power mask is slightly displaced to low frequencies. A correction to high frequencies of around 20 kHz must be introduced in each notch definition to compensate this effect. The notches of the IARU power mask are also calculated and they are also displaced. As a result of this displacement, two of the notches included in IARU regulation are a few dB less attenuated than required.

Number of hops in Time Division Domains

The number of hops supported in a Time Division Domain is ten. In networks were more hops are needed, it is recommended to use several Frequency Division Domains.

ANNEX 2: EXAMPLE OF CONFIGURATION FILES

Master Access Mode 6 (HE/LV 6) output to coaxial port

GENERAL_USE_AUTOCONF = YES
GENERAL_TYPE = HE GENERAL_FW_TYPE = LV
GENERAL_IP_ADDRESS = 192.168.0.100
GENERAL_IP_NETMASK = 255.255.255.0
GENERAL_IP_GATEWAY = 192.168.0.1
GENERAL_IP_USE_DHCP = YES
GENERAL_STP = YES
GENERAL_AUTHENTICATION = NONE
GENERAL_SIGNAL_MODE = 6
SIGNAL_SUB_MODE = 0
GENERAL_SIGNAL_REG_POWER_MASK_ENABLE = NO
PLC_SIGNAL_COUPLING = COAX

Master Access Mode 1 (HE/LV 1) output to pin 3 and 4

GENERAL_USE_AUTOCONF = YES
GENERAL_TYPE = HE GENERAL_FW_TYPE = LV
GENERAL_IP_ADDRESS = 192.168.0.100
GENERAL_IP_NETMASK = 255.255.255.0
GENERAL_IP_GATEWAY = 192.168.0.1
GENERAL_IP_USE_DHCP = YES
GENERAL_STP = YES
GENERAL_AUTHENTICATION = NONE
GENERAL_SIGNAL_MODE = 1
SIGNAL_SUB_MODE = 0
GENERAL_SIGNAL_REG_POWER_MASK_ENABLE = NO
PLC_SIGNAL_COUPLING = LV

Master Access Mode 2 (HE/LV 2) output to pin 3 and 4

GENERAL_USE_AUTOCONF = YES
GENERAL_TYPE = HE
GENERAL_FW_TYPE = LV
GENERAL_IP_ADDRESS = 192.168.0.100
GENERAL_IP_NETMASK = 255.255.255.0
GENERAL_IP_GATEWAY = 192.168.0.1
GENERAL_IP_USE_DHCP = YES
GENERAL_STP = YES
GENERAL_AUTHENTICATION = NONE
GENERAL_SIGNAL_MODE = 2
SIGNAL_SUB_MODE = 0
GENERAL_SIGNAL_REG_POWER_MASK_ENABLE = NO
PLC_SIGNAL_COUPLING = LV

Master Access Mode 3 (HE/LV 3) output to pin 3 and 4

GENERAL_USE_AUTOCONF = YES
GENERAL_TYPE = HE
GENERAL_FW_TYPE = LV
GENERAL_IP_ADDRESS = 192.168.0.100
GENERAL_IP_NETMASK = 255.255.255.0
GENERAL_IP_GATEWAY = 192.168.0.1
GENERAL_IP_USE_DHCP = YES
GENERAL_STP = YES
GENERAL_AUTHENTICATION = NONE
GENERAL_SIGNAL_MODE = 3
SIGNAL_SUB_MODE = 0
GENERAL_SIGNAL_REG_POWER_MASK_ENABLE = NO
PLC_SIGNAL_COUPLING = LV

Slave End User (CPE/EU) output to pin 3 and 4

GENERAL_USE_AUTOCONF = YES
GENERAL_TYPE = CPE
GENERAL_FW_TYPE = EU
GENERAL_IP_ADDRESS = 192.168.0.101
GENERAL_IP_NETMASK = 255.255.0.0
GENERAL_IP_GATEWAY = 192.168.0.1
GENERAL_IP_USE_DHCP = YES
GENERAL_STP = YES
GENERAL_SIGNAL_MODE_LIST.1 = 1
GENERAL_SIGNAL_MODE_LIST.2 = 2
GENERAL_SIGNAL_MODE_LIST.3 = 3
GENERAL_SIGNAL_MODE_LIST.4 = 6
GENERAL_SIGNAL_MODE_LIST.5 = 7
GENERAL_SIGNAL_MODE_LIST.6 = 8
GENERAL_SIGNAL_MODE_LIST.7 = 10
GENERAL_SIGNAL_MODE_LIST.8 = 13
GENERAL_SIGNAL_REG_POWER_MASK_ENABLE = NO
PLC_SIGNAL_COUPLING = LV

TD Repeater (TDR/LV) output to pin 3 and 4

GENERAL_USE_AUTOCONF = YES
GENERAL_TYPE = TDREPEATER
GENERAL_FW_TYPE = LV
GENERAL_IP_ADDRESS = 192.168.0.103
GENERAL_IP_NETMASK = 255.255.0.0
GENERAL_IP_GATEWAY = 192.168.0.1
GENERAL_IP_USE_DHCP = YES
GENERAL_STP = YES
GENERAL_SIGNAL_MODE_LIST.1 = 1
GENERAL_SIGNAL_MODE_LIST.2 = 2

GENERAL_SIGNAL_MODE_LIST.3 = 3
GENERAL_SIGNAL_MODE_LIST.4 = 6
GENERAL_SIGNAL_MODE_LIST.5 = 7
GENERAL_SIGNAL_MODE_LIST.6 = 8
GENERAL_SIGNAL_MODE_LIST.7 = 10
GENERAL_SIGNAL_MODE_LIST.8 = 13
GENERAL_SIGNAL_REG_POWER_MASK_ENABLE = NO
PLC_SIGNAL_COUPLING = LV

Master Access Mode 6 (HE/LV 6) with VLAN and OVLAN parameters

GENERAL_USE_AUTOCONF = YES
GENERAL_TYPE = HE
GENERAL_FW_TYPE = LV
GENERAL_IP_ADDRESS = 192.168.0.100
GENERAL_IP_NETMASK = 255.255.255.0
GENERAL_IP_GATEWAY = 192.168.0.1
GENERAL_IP_USE_DHCP = YES
GENERAL_STP = YES
GENERAL_AUTHENTICATION = AUTHLIST
GENERAL_SIGNAL_MODE = 6
GENERAL_SIGNAL_REG_POWER_MASK_ENABLE = NO
PLC_SIGNAL_COUPLING = LV

SIGNAL_SUB_MODE = 0

TRANSLATION_MNMT_VLAN = 5
TRANSLATION_DATA_VLAN.1 = 101
TRANSLATION_DATA_VLAN.2 = 102
TRANSLATION_ROOTPATH_OVLAN = 77

QOS_ENABLE = YES
QOS_BW_POLICY = 1

COS_CRITERION.1 = TCP_8021p

OVLAN_ENABLE = YES
OVLAN_DATA_TAG = 4095

PROFILE_MAX_TXPUT_TX.1 = 4096
PROFILE_MAX_TXPUT_RX.1 = 4096
PROFILE_PRIORITIES.1 = 0xFF
PROFILE_UPBWLIMIT.1 = NO
PROFILE_DWBWLIMIT.1 = NO
PROFILE_MNMT_VLAN.1 = %MNMT
PROFILE_FWTYPE.1 = EU

PROFILE_MAX_TXPUT_TX.2 = 512
PROFILE_MAX_TXPUT_RX.2 = 1024
PROFILE_PRIORITIES.2 = 0xFF
PROFILE_UPBWLIMIT.2 = NO
PROFILE_DWBWLIMIT.2 = NO
PROFILE_MNMT_VLAN.2 = %MNMT
PROFILE_DATA_VLAN.2 = %DATA1
PROFILE_FWTYPE.2 = EU

PROFILE_MAX_TXPUT_TX.3 = 1024
PROFILE_MAX_TXPUT_RX.3 = 2048
PROFILE_PRIORITIES.3 = 0xFF
PROFILE_UPBWLIMIT.3 = NO
PROFILE_DWBWLIMIT.3 = NO
PROFILE_MNMT_VLAN.3 = %MNMT
PROFILE_DATA_VLAN.3 = %DATA2
PROFILE_FWTYPE.3 = EU

#Users must place the MAC address of CPE modems here.
ACCESSP_AUTHLIST_MAC.1 = 0x000BC2XXXXXX
ACCESSP_AUTHLIST_PROFILE.1 = 2
ACCESSP_AUTHLIST_MAC.2 = 0x000BC2XXXXXX
ACCESSP_AUTHLIST_PROFILE.2 = 3

Slave End User (CPE/EU) with VLAN 101 and OVLAN parameters

GENERAL_USE_AUTOCONF = YES
GENERAL_TYPE = CPE
GENERAL_FW_TYPE = EU
GENERAL_IP_ADDRESS = 192.168.0.102
GENERAL_IP_NETMASK = 255.255.255.0
GENERAL_IP_GATEWAY = 192.168.0.1
GENERAL_IP_USE_DHCP = YES

GENERAL_STP = YES

GENERAL_SIGNAL_MODE_LIST.1 = 1
GENERAL_SIGNAL_MODE_LIST.2 = 2
GENERAL_SIGNAL_MODE_LIST.3 = 3
GENERAL_SIGNAL_MODE_LIST.4 = 6
GENERAL_SIGNAL_MODE_LIST.5 = 7
GENERAL_SIGNAL_MODE_LIST.6 = 8
GENERAL_SIGNAL_MODE_LIST.7 = 10
GENERAL_SIGNAL_MODE_LIST.8 = 13
GENERAL_SIGNAL_REG_POWER_MASK_ENABLE = NO
PLC_SIGNAL_COUPLING = LV

QOS_ENABLE = YES
QOS_MAX_TXPUT_TX = 2048

VLAN_MNMT_TAG = %MNMT
VLAN_DATA_TAG = %DATA1
VLAN_DATA_PRIO = 4

OVLAN_ENABLE = YES
OVLAN_DATA_TAG = %ROOTPATH

Slave End User (CPE/EU) with VLAN 102 and OVLAN parameters

GENERAL_USE_AUTOCONF = YES
GENERAL_TYPE = CPE
GENERAL_FW_TYPE = EU
GENERAL_IP_ADDRESS = 192.168.0.102
GENERAL_IP_NETMASK = 255.255.255.0
GENERAL_IP_GATEWAY = 192.168.0.1
GENERAL_IP_USE_DHCP = YES
GENERAL_STP = YES

GENERAL_SIGNAL_MODE_LIST.1 = 1
GENERAL_SIGNAL_MODE_LIST.2 = 2
GENERAL_SIGNAL_MODE_LIST.3 = 3
GENERAL_SIGNAL_MODE_LIST.4 = 6
GENERAL_SIGNAL_MODE_LIST.5 = 7
GENERAL_SIGNAL_MODE_LIST.6 = 8
GENERAL_SIGNAL_MODE_LIST.7 = 10
GENERAL_SIGNAL_MODE_LIST.8 = 13
GENERAL_SIGNAL_REG_POWER_MASK_ENABLE = NO
PLC_SIGNAL_COUPLING = LV

QOS_ENABLE = YES
QOS_MAX_TXPUT_TX = 2048

VLAN_MNMT_TAG = %MNMT
VLAN_DATA_TAG = %DATA2
VLAN_DATA_PRIO = 4

OVLAN_ENABLE = YES
OVLAN_DATA_TAG = %ROOTPATH